シュプリンガー数学クラシックス　第18巻

P.サミュエル［著］
織田 進［訳］

数の代数的理論

Springer
シュプリンガー・フェアラーク東京

Translation from the French language edition:
Théorie Algébrique des Nombres by P. Samuel

はじめに

数論または算術は「数学の女王」とよくいわれる．対象とするもの（整数やそれの一般化）の単純性，その方法の簡潔さや多様さ，その多くの未解決の問題はすべての領域の数学者を強く魅了する．たとえ彼らが初心者であれ，数論の専門家であれ，または数学の他の分野のスペシャリストであったとしてもそうである．著者が代数幾何学者であって，整数論とよばれるにふさわしい独創的研究を1つも発表したことがないことを読者が知ったとしても，そんなに驚くべきではないだろう．

従って，本書は数論についての特別深遠なまたは包括的な取り扱いを期待されるものではない．さらにいえば，数論へ近づく多くの方法のうちの1つ，すなわち，代数的方法だけを含んでいる．$\mathbb{R}^n$ における格子に関する Minkowski の初等的結果を除けば，解析的数論の美しく豊穣な方法は本書ではまったく省略されている．

代数的方法を強調することはいくつかの理由で正当化されると思われる．まずはじめに，それは数論の問題が最も自然に定式化されるところへ迅速に行けることである．これは自然数のみに関連する問題において特にあてはまる．たとえば，Pell-Fermat の方程式 $X^2 - dY^2 = \pm 1$（d は平方数でない）のすべての整数解を見つける問題は本質的な意味で2次体 $\mathbb{Q}(\sqrt{d})$ の研究を含んでいる．Fermat の「偉大な」方程式 $X^n + Y^n = Z^n$ に対しては，1の n 乗根の体が類似の役割を演ずる．整数を2つ（あるいは，4つ）の平方数の和として表すためには，Gauss の整数環 $\mathbb{Z}[i]$（あるいは，うまく選ばれた四元数環）において考えるのが有利である．平方剰余の相互法則は，2次体

と1のべき根を必要とする．上にあげた問題のどれを考察するにも，有理数体 $\mathbb{Q}$ よりも一般的な体や，整数環 $\mathbb{Z}$ よりも一般的な環，また $\mathbb{Z}$ の剰余体，すなわち，有限体とそれ上の代数などがごく自然に現れてくる．

また，代数的な方法がすべての数論をカバーするものではないとしても，後にわかるように，それは早急に充実した結果をもたらしてくれる．本書のもつこの方向を継続することによって，類体論というような深い定理に到達するであろう．

次に，解析的方法を好む人々でも，その大いなる一般性と威力はもっぱら代数体や単純環に応用するときに現れるのであって，$\mathbb{Q}$ のみを探求するときではないことは認めるであろう．たとえば，数体 K の Dedekind のゼータ関数 $\zeta_K(s)$ や L-級数を同時に扱うことなしで，Riemann のゼータ関数 $\zeta(s)$ のみを研究しようとすることは，そう有意義ではないであろう．

代数的方法を展開することは，代数の授業で出会う概念 —— 群，環，体，イデアル，剰余環と剰余体，準同型と同型，加群とベクトル空間 —— を説明する，夥しい数の例を学生に見せてくれる．学生にとってさらに有益なことは，代数的数論を学ぶことにより，多くの新しい代数的概念，それは数論のみでなく，他の数学の分野，とりわけ代数幾何のための基礎的概念に出会えるという点である．いくつかの例をあげると，環上の整元，体の拡大，Galois 理論，単項イデアル環上の加群，Noether 環と加群，Dedekind 環，そして分数環がある．

以上で，読者が本書で何を見いだし何を見いださないことになるかについての概略を述べてきた．著者は本書の読者に対し次のような基礎的代数学は既知のものとして仮定している —— 群，環，多項式環，ベクトル空間に関する初歩的事実 —— これらのカテゴリーでの部分対象，剰余対象，積対象 —— イデアルや加群による剰余に移るメカニズム —— 射と同型射のいろいろな概念．読者はこれらのすべて（そして必要以上）については「現代」的といわれる代数学の基本的なテキストの中で見いだすことができる．たとえば，R. Godement (Houghton-Mifflin) や S. Lang (Addison-Wesley) の優れたテキストがある．本書では全般を通して，「現代」代数学のことばと結果を用いており，読者の便宜のために，次のような概念の議論，環上の整元，体の拡大，Galois 理論，Noether 環と加群，分数環，については記述しておいた．これ

らのトピックスは短くかつ明白に，ただし不必要に洗練することなしに，説明を与えるように努めた．

本書は，1965 年と 1966 年に繰り返しおこなったパリ大学での「高等数学」という講義内容をもとにしている．École Normale Supérieure の学生である Alfred Vidal-Madjar によってとられたコースノートが第 1 稿として提供された．彼に対して心からの謝辞を表したい．ある部分はÉcole Normale Supérieure de Jeunes Filles と Clermont-sur-Tiretaine 大学で講義したコースに由来する．最後に，何人かの数学者からの影響と助言は有意義であった．とりわけ未発表の原稿を親切にも見せてくれた，著者の世代の先生，N. Bourbaki に特に感謝を申し上げたい．また，友人 Emil Grosswald，Georges Poitou，Jean-Pierre Serre と John Tate に特別の感謝を表したい．

第 2 版の前書き

初版への数知れない読者に心からの感謝を捧げる．特に Germaine Revuz，Alain Bouvier と Pierre Cartier，彼らは誤りについての有益なリストを作ってくれた．英語版の訳者である Allan Silberger にも御礼申し上げる．

1971 年 7 月 著　者

À NICOLE
qui a su créer autour de moi
une atmosphère favorable à ce livre

記号，定義，予備知識

集合論で通常用いられている記号 $\in, \subset, \cup, \cap$ を用いる．集合 A における部分集合 B の補集合 (complement) を $A \setminus B$ と表し，$\emptyset$ は空集合 (empty set) を表す．集合 A の濃度 (cardinality) （または，元の個数）を $\mathrm{card}(A)$ と表し，もし A が群のときは，それを A の位数 (order) という．

群 (group)，環 (ring)，体 (field) を含めて，ベクトル空間の初歩理論（「線型代数 (linear algebra)」ともいわれる）は既知であると仮定する．本書においては，5.7 節を除いて，「環」（あるいは，「体」）は可換環（あるいは，可換体）で単位元をもつものとする．

有限群 (finite group) G とその部分群 (subgroup) H が与えられたとき，$\mathrm{card}(H)$ は $\mathrm{card}(G)$ を整除することを思い出そう．商 $\mathrm{card}(G)/\mathrm{card}(H)$ は H の G における指数 (index) といわれ，$(G : H)$ と表される．

加法群 (additive group) G の 2 つの部分群 A と B が与えられたとき，和 $a + b$ $(a \in A, b \in B)$ の全体の集合を $A + B$ と表す．

A を環とするとき，A 上 1 変数 (variable) の多項式 (polynomial) のなす環を $A[X]$ または $A[Y]$ （大文字）と表し，n 変数 $X_1, \ldots, X_n$ の多項式に対しては $A[X_1, \ldots, X_n]$ と表し，変数 X の形式的べき級数 (formal power series) のなす環を $A[[X]]$ と表す．

慣例として，環 B の部分環 (subring) A は B の単位元を含むものとする．環 B とその部分環 A と元 x が与えられたとき，A と x で生成された B の部分環を $A[x]$ と表す．これは A と x を含む B のすべての部分環の共通部分であり，$a_0 + a_1 x + \cdots + a_n x^n$ $(a_i \in A)$ の形で表されるすべての集合で

ある．同様に A と B の元の有限集合 $\{x_1,\dots,x_n\}$ で生成される B の部分環を $A[x_1,\dots,x_n]$ と表す．

環 A は，1 元以上を含みかつ A の任意の 0 でない 2 つの元の積 (product) が 0 でないとき，整域 (integral domain) であるといわれる．

環 A のイデアル (ideal) $\mathfrak{b}$ とは，$x\in\mathfrak{b}$ と $a\in A$ に対して $ax\in\mathfrak{b}$ が成り立つような A の加法群の部分群のことである．環全体，元 0 のみからなる集合（これを (0) と表す）は，イデアルであり，しばしば「自明な」イデアルとよぶ．体は自明でないイデアルをもたない環である．環 A の元の集合 $\{b_i\}$ が与えられたとき，すべての b_i を含む A の任意のイデアルの共通部分は，$\{b_i\}$ で生成されたイデアルといわれ，それは $\sum_i a_ib_i$ $(a_i\in A)$ の形の元全体からなる集合である．唯 1 つの元 $b\in A$ で生成されたイデアルは単項イデアル (principal ideal)（または，主イデアル）といわれ，記号 Ab または (b) と表される．

A を環，$\mathfrak{b}$ を A のイデアルとする．同値類 (equivalence class) $a+\mathfrak{b}$ $(a\in A)$ 全体は環をなす．これを A の $\mathfrak{b}$ による剰余環 (quotient ring) といい，$A/\mathfrak{b}$ と表す．$x,y\in A$ が $x-y\in\mathfrak{b}$ のとき，x と y は**合同**であるといい，$x\equiv y \pmod{\mathfrak{b}}$ と表す．また x と y は $\mathfrak{b}$ を**法**として等しいともいう．$A/\mathfrak{b}$ のすべてのイデアルは $\mathfrak{b}'/\mathfrak{b}$ の形である．ここで $\mathfrak{b}'$ は $\mathfrak{b}$ を含む A のイデアルの集合の中を動く．$A/\mathfrak{b}$ が体であるための必要十分条件は，$\mathfrak{b}$ が A と異なる A のイデアル全体の中で極大であることである．このとき，$\mathfrak{b}$ は極大イデアル (maximal ideal) であるという．イデアル $\mathfrak{p}$ は $A/\mathfrak{p}$ が整域であるとき，素イデアル (prime ideal) であるといわれる．

A と A' が環で，e と e' をそれぞれの単位元とする．準同型 (homomorphism) $f: A\to A'$ は A から A' への写像 (mapping) f で，

$$f(a+b)=f(a)+f(b),\quad f(ab)=f(a)f(b),\quad f(e)=e'$$

となるものである．

A を環とする．A-代数 (algebra) とは環 B と準同型 $\varphi: A\to B$ の組 (B,φ) のことである．（単に A-代数 B ということが多い．）A が体ならば，φ は単射 (injection) で，このとき A とその像 (image) $\varphi(A)$（これは B の部分環）をしばしば同一視する．

体 L とその部分体 K が与えられたとき，L は K の拡大 (extension) といわれる．

通常，環 A の単位元は 1 と表される．

環 A 上の加群 (module)（または A-加群）の概念は，体上のベクトル空間の概念の直接的一般化である．A-加群 M とは，Abel 群（加法）で，写像 $A \times M \to M$（(a, x) に ax を対応させる）であって，$a(x+y) = ax + ay$, $(a+b)x = ax + bx$, $a(bx) = (ab)x$, $1x = x$ $(a, b \in A,\ x, y \in M)$ が成り立つものを備えているものをいう．A-部分加群 (A-submodule)，A-剰余加群 (A-quotient module) が考えられる．A-加群 M と M' に対して，M から M' への準同型（または，A-線型写像）とは写像 $f : M \to M'$ で

$$f(x+y) = f(x) + f(y),\ f(ax) = af(x),\ (a \in A,\ x, y \in M)$$

をみたすものである．

群（あるいは，環，加群）の準同型 $f : X \to X'$ に対して，f による 1（あるいは，0）の逆像を f の核 (kernel) とよび，$\mathrm{Ker}(f)$ と表す．これは X の正規部分群（あるいは，イデアル，部分加群）となる．f が単射であるための必要十分条件は $\mathrm{Ker}(f) = \{1\}$（あるいは，$\{0\}$ ）となることである．X' の部分集合 $f(X)$ を f の像 (image) という．これは X' の部分群（あるいは，部分環，部分加群）である．

X と X' を集合とする．X から X' への写像を常に $f : X \to X'$ と表す．写像 $f : X \to X'$ が任意の $x \in X$ のとる値によって表されるとき，$x \mapsto f(x)$ という表現を使う．従って，正弦関数 (sine function)，$\sin : \mathbb{R} \to \mathbb{R}$ は

$$x \mapsto \sum_{n=0}^{\infty} (-1)^n \frac{x^{2n+1}}{(2n+1)!}$$

と定義することができる．

次のようなよく用いられる記号を採用する．

$\mathbb{N}$：自然数全体の集合 $\{0, 1, 2, \ldots, n, \ldots\}$ ....（“number”の N）

$\mathbb{Z}$：（有理）整数全体のなす環

（自然数とその反数を含む）......................（“Zahlen”の Z）

$\mathbb{Q}$：有理数全体のなす体（$\mathbb{Z}$ の商体） ....（“quotient”の Q）

$\mathbb{R}$：実数全体のなす体 .... （"real"の R）
$\mathbb{C}$：複素数全体のなす体 .... （"complex"の C）
$\mathbb{F}_q$：q 個の元からなる有限体 .... （"finite"または "field"の F）

各章末にある練習問題は，より手間のかかる問題には問題番号に*をつけ，本書の理解をチェックするためのやさしい問題と区別した．

この訳書（原著もそうであるが）において，次のことを注意しておこう．

「K を体，z を K 上代数的な元とするとき，体としての拡大 $K(z)$ と環としての拡大 $K[z]$ は等しい.」

実際，$K(z)$ は K と z を含む体の中で最小のものと定義される．$K[z] \subseteq K(z)$ は明らかである．よって $K[z]$ が体になることを示せばよい．z の K 上の最小多項式を $f(x) \in K[X]$ とするとき，$K[z]$ は z が K 上代数的であることより $(f(x)) \neq (0)$ である．$f(x)$ は $K[X]$ において既約式であるから，イデアル $(f(x))$ は素イデアルであるが，極大イデアルであることも容易にわかる．よって $K[z] \cong K[X]/(f(x))$ は体である．これで「　」の記述が成り立つことが示された．

目　次

第I章　単項イデアル環

1.1　単項イデアル環における整除

A を整域，K をその分数体，x と y を K の元とする．ある $a \in A$ が存在して，$y = ax$ となるとき，x は y を**整除する**という．同値なことだが，x は y の**約元**，y は x の**倍元**といい，$x|y$ と表す．K の元の間のこの関係は本質的に環 A に依存する．もし，何らかの混乱があり得るときは，A に関する K における整除ということにする．

$x \in K$ が与えられたとき，x の倍元のなす集合を Ax と表す．よって，$x|y$ の代わりに $y \in Ax$ と表してもよく，これはまた $Ay \subset Ax$ とも書ける．集合 Ax は K の A に関しての**単項分数イデアル** (principal fractional ideal) とよばれる．もし $x \in A$ ならば，Ax は（通常の）x で生成された A の単項イデアルである．整除の関係として，$x|y$ は順序関係 $Ay \subset Ax$ と同値であり，整除は順序関係に付随した次の 2 つの性質をもっている．

$$x|x \text{ である，さらに } x|y \text{ かつ } y|z \text{ ならば } x|z \text{ である．} \tag{1}$$

他方，$x|y$ かつ $y|x$ ならば $x = y$ と結論することは一般にはできない．ただ，$Ax = Ay$ となるだけである．これは（もし $y \neq 0$ ならば）商 xy^{-1} が A の可逆元であることを意味する．このとき，x と y は**同伴** (associated) であるという．これらは整除の立場から見れば，区別がつかない．

∞ **例**．K の元で 1 に同伴なものは A においてすべて可逆な元である．これら

はしばしば A における**単元**とよばれる．そして，それらは乗法の下で群をなし A^* と表される．環 A の単元 の決定は興味深い問題であり，後に A が数体 (number field) の整数環 (ring of integers) の場合を取り扱う（第 IV 章を参照）．ここではいくつかの簡単な例をあげる．

(a) A が体ならば $A^* = A \setminus \{0\}$.

(b) $A = \mathbb{Z}$ ならば $A^* = \{+1, -1\}$.

(c) A が整域のとき，多項式環 $B = A[X_1, \ldots, X_n]$ の単元全体は可逆な定数全体，言い換えれば，$B^* = A^*$ である．

(d) 形式的べき級数環 $A[[X_1, \ldots, X_n]]$ の単元全体は，定数項が可逆な形式的べき級数全体である．

定義 1. 環 A が整域で，そのすべてのイデアルが単項イデアルであるとき，A を**単項イデアル環** (principal ideal ring) という．

有理整数 $\mathbb{Z}$ は単項イデアル環である（$\mathbb{Z}$ の任意のイデアル $\mathfrak{a} \neq (0)$ は最小の整数 $b > 0$ を含む．$x \in \mathfrak{a}$ を b で割ると，$\mathbb{Z}$ が Euclid 環であることより，x は b の倍数である）．K を体とすれば，1 変数多項式環 $K[X]$ は単項イデアル環である（同様な証明による，すなわちイデアル $\mathfrak{a} \neq (0)$ の中で 0 でない最小次数の多項式を $b(X)$ として，$K[X]$ が Euclid 環であること，すなわち，$\mathfrak{a}$ の任意の元を $b(X)$ で割ったときの剰余は $b(X)$ の次数より小さな次数でなければならない）．この一般的な方法により，任意の Euclid 環（[1，第 VIII 章，§1]，または [9，第 I 章] を参照）は単項イデアル環である．K が体ならば，形式的べき級数環 $A = K[[X]]$ の 0 でない任意のイデアルは AX^n $(n \geq 0)$ の形であり，従って，A も単項イデアル環である．

単項イデアル環 A の分数体 K における整除は特別に簡単である．手短に見ておこう．

I. 2 つの任意の元 $u, v \in K$ に対して，**最大公約元** (the greatest common divisor) $\mathrm{GCD}(u, v) = d$ をもつ．すなわち，関係

$$「x|u \text{ かつ } x|v」 \quad と \quad 「x|d」 \tag{1}$$

が同値であるような元 d をもつ．これは分数イデアルの半順序集合において，

Au と Av が最小上界 (the least upper bound) をもつことと同じことを意味する．この最小上界は $Au + Av$ であり，それ自身，単項イデアルである（これは $u, v \in A$ なら明らかであり，$u, v \in K$ ならば共通分母を掛けることによって，前者に帰着する）．補足的に次のことがいえる（「Bezout の等式」），つまり u, v の最大公約元は $a, b \in A$ を適当にとって，

$$d = au + bv \tag{2}$$

の形に書き表せる．u, v の最大公約元は A の単元の積を度外視すれば，明らかに唯 1 つ定まる．

II. 2 つの任意の元 $u, v \in K$ に対して，**最小公倍元** (the least common multiple) $\mathrm{LCM}(u, v) = m$ をもつ．すなわち，関係

$$「\ u|x \quad \text{かつ} \quad v|x\ 」 \qquad \text{と} \qquad 「\ m|x\ 」 \tag{3}$$

が同値であるような元 $m \in K$ をもつ．これは，K において $t \mapsto t^{-1}$ の対応が整除を逆にすることよりわかる．従って，最小公倍元の存在の証明は最大公約元の存在の証明に還元される．関係

$$\mathrm{LCM}(u, v) = \mathrm{GCD}(u^{-1}, v^{-1})^{-1} \qquad (u, v \neq 0) \tag{4}$$

より，次の公式が容易に導かれる．

$$\mathrm{GCD}(u, v) \cdot \mathrm{LCM}(u, v) = uv. \tag{5}$$

I と同様にして，$\mathrm{LCM}(u, v)$ の存在は，単項分数イデアルの半順序集合において，Au と Av の最大下界 (the greatest lower bound) の存在と同値である．Au と Av の最大下界は $Au \cap Av$ である．

III. 2 つの A の元 a, b は $\mathrm{GCD}(a, b) = 1$ のとき，**互いに素** (relatively prime, co-prime) といわれる．重要な Euclid の補題を復習しておこう．a, b, c を単項イデアル環 A の元とする．a が，bc を割り切り，b と互いに素であれば，a は c を割り切る．

⚮ Euclid の補題の手早い証明．Bezout の等式 (2) により，$1 = a'a + b'b$ と

なる元 $a', b' \in A$ がある．よって，$c = a'ac + b'bc$. a はこの右辺の 2 項を割り切るから，a は c を割り切る．

IV. 最後に，重要な**素元の積への分解**について述べておこう．

定理. A を単項イデアル環，K をその分数体とする．素元からなる A の部分集合 P があって，任意の $x \in K$ は

$$x = u \prod_{p \in P} p^{v_p(x)} \tag{6}$$

の形に一意的に表される．ここで，u は A の可逆元，指数 $v_p(x)$ は $\mathbb{Z}$ の元で有限個の $p \in P$ を除いて 0 である．

∞ これについてのもっと組織だった表現については [1，第 VI 章，§1 および第 VII 章，§1] を参照せよ．この理論の一部（より正確には，Bezout の等式に依存しないものすべて）は単項イデアル環よりもっと一般の環に拡張される．一意分解整域（unique factorization domain または factorial ring）について参照できるだろう（[7] または [2，第 VII 章，§3] を参照）．

1.2　方程式 $X^2 + Y^2 = Z^2$ と $X^4 + Y^4 = Z^4$

数論の最も魅力的な分野の 1 つとして，Diophantus 方程式 (Diophantine equation) の研究がある．$\mathbb{Z}$（あるいは，$\mathbb{Q}$）に係数をもつ多項式方程式 $P(X_1, \ldots, X_n) = 0$ を考え，$\mathbb{Z}$（あるいは，$\mathbb{Q}$）における解 (x_i) を探すのである．$\mathbb{Z}$（あるいは，$\mathbb{Q}$）をより一般的な環 A（あるいは，体 K）で置き換えることもできる．後（1.6 節）に例を与える．

ここでは Fermat の有名な方程式，

$$X^n + Y^n = Z^n \tag{1}$$

の特別な場合を考えることにする．Fermat は，$n \geq 3$ に対してはこの方程式は自明でない整数解 (x, y, z) は存在しないことを証明したと主張した．彼の証明は不明のままである．Fermat の時代から，たくさんの数学者が精力的にこの問題に携わってきた．非常に多くの指数 n の値について Fermat の

主張が正しいことが示されてきた．それでもなお，一般証明（すなわち，任意の n に対して成り立つ）は見いだされていない*.

∞ 現在では，Fermat は「証明」の中で誤りをした，しかし一級の数学者に値する誤りであったということになっている．たとえば，1 の n 乗根を含む体の整数環において何かするという考え（彼の時代では巧妙であったが）を抱いていたと思われる．彼はそのような環は常に単項イデアル環であると信じていたのであろう．実際，1 の n 乗根の環が単項イデアル環であるような指数 n について，Fermat の主張を証明する方法は知られている．けれども，すべての n に対してこれらがあてはまるわけではない．素数 n に対して，この環が単項イデアル環になるのは，n が有限個の値のときに限られる†.

$n=2$ のときは，方程式 (1) は整数解，たとえば (3, 4, 5) をもち，さらに (1) のすべての整数解について完全に記述することができる．

定理 1. x,y,z を $x^2+y^2=z^2$ が成り立つ正の整数とすると，ある整数 d と 2 つの互いに素な整数 u,v が存在して，(x と y の入れ換えを除けば)

$$x=d(u^2-v^2), \quad y=2duv, \quad z=d(u^2+v^2) \tag{2}$$

と表せる．

証明 (2) の x,y,z が $X^2+Y^2=Z^2$ の解であることは簡単な計算でわかる．逆に，x,y,z が正の整数で $x^2+y^2=z^2$ となるものとする．x,y,z の最大公約数で割ることにより，この 3 つの数は互いに素と仮定してよい．このとき，これらのどの 2 つも互いに素である．たとえば，x,y が素数の公約数 p をもつとすると，p は $y^2=z^2-x^2$ を割り切り，よって y も割り切る．特に x,y,z の 2 つは奇数であるが，3 つ目のものは必然的に偶数である．x と y はともに奇数とはなり得ない．なぜならば，もしそうだとすると，$x^2\equiv 1 \pmod 4$, $y^2\equiv 1 \pmod 4$, $z^2\equiv 2 \pmod 4$ となり，これは z^2 が平方数であることに矛盾する．従って，x,y を入れ換えることが可能であることより，

$$x \text{ 奇数}, \quad y \text{ 偶数}, \quad z \text{ 奇数} \tag{3}$$

---

* ［訳注］A. Wiles が最終結果を証明した．論文 Modular elliptic curves and Fermat last theorem, Ann. of Math., **142**(1995), 443–551.

† C. L. Siegel, *Gesammelte Werke*, Part III, pp. 436–442.

となる．

$$y^2 = z^2 - x^2 = (z-x)(z+x) \tag{4}$$

が成り立つことに注意する．$2x$ と $2z$ の最大公約数は 2 で，$2x = (z+x)-(z-x)$, $2z = (z+x)+(z-x)$ であるから，$z-x$ と $z+x$ の最大公約数は 2 のみである．$y = 2y'$, $z+x = 2x'$, $z-x = 2z'$ とおく．ここで，x', y', z' は整数である（y, $z+x$, $z-x$ は (3) より偶数であるから）．よって，$y'^2 = x'z'$ となる．x' と y' は互いに素であるから，x' と y' は平方数 u^2 と v^2 である．実際，y^2 の任意の素因数は偶数指数をもつ形で，x' または z' の素因数分解のどちらかに現れるが，両方ではない．よって $z+x = 2u^2$, $z-x = 2v^2$, $y^2 = 2u^2 \cdot 2v^2$ であることより，$x = u^2 - v^2$, $y = 2uv$, $z = u^2 + v^2$ となる．ここで，u と v は互いに素である．なぜならば，もしそうでないとすると，x, y, z は自明でない公約数をもってしまうからである．元々の x, y, z の最大公約数を d として，それを掛けることによって (2) を得る．□

定理 2. 方程式 $X^4 + Y^4 = Z^2$ は正の整数 x, y, z を解としてもたない．

証明　背理法で示す．解 $(x,\ y,\ z)$ があったとすると，z が最小であるようなものがある．このとき x, y, z はどの 2 つも互いに素である．たとえば，x, y が素数の公約数 p をもてば，p^4 は z^2 を割り切り，結局 p^2 は z を割り切ることになり，$(x/p,\ y/p,\ z/p^2)$ が解になってしまう．これは z の最小性に矛盾する．他の 2 つの場合も同様であり，かえって容易である．方程式は $(X^2)^2 + (Y^2)^2 = Z^2$ と表されるから，これに定理 1 を適用する．必要なら，x, y を入れ換えることにして，互いに素な正の整数 u, v があって，

$$x^2 = u^2 - v^2, \quad y^2 = 2uv, \quad z = u^2 + v^2 \tag{5}$$

と書ける．$4|y^2$ であるから，$y^2 = 2uv$ の関係により u または v の一方は偶数であり，他方は必然的に奇数となる．よって，u は偶数，v は奇数とすると $u^2 \equiv 0 \pmod 4, v^2 \equiv 1 \pmod 4$ となる．ここで $x^2 = u^2 - v^2 \equiv -1 \pmod 4$ となり，これは不可能である．ゆえに u は奇数で $v = 2v'$ となる．$y^2 = 4uv'$ であることと u と v が互いに素であることより，u と v' は平方数 a^2 と b^2 である．定理 1 を再度用いる，今回は方程式 $x^2 + v^2 = u^2$（(5) を参照）．x

と u は奇数，v は偶数で，x, v, u はどの 2 つも互いに素であることより，互いに素な整数 c と $d \geq 1$ で

$$x = c^2 - d^2, \quad v = 2cd, \quad u = c^2 + d^2 \tag{6}$$

となるものがある．ところで，$v = 2v' = 2b^2$ より，$cd = b^2$ がいえて，c と d は互いに素だから再び平方数 x'^2 と y'^2 になる．$u = a^2$ であることより (6) の最後の等式は

$$a^2 = x'^4 + y'^4 \tag{7}$$

の形に書き換えてよい．これは元々の方程式と同じ形である．一方，(5) により $z = u^2 + v^2 = a^4 + 4b^4 > a^4$ であるから $z > a$ となる．これは z の最小性に矛盾する．これで定理 2 の証明は終わる． □

☞ この証明を少し変えることにより，もし $X^4 + Y^4 = Z^2$ の正の整数解が得られたら，このような無限個の解の列 (x_n, y_n, z_n)（ここで $\{z_n\}$ は真に減少していく）を構成できることになり，不合理であるということになる．こういう証明の方法は**無限降下法**とよばれ，Fermat によるものである．

系．方程式 $X^4 + Y^4 = Z^4$ は正の整数解をもたない．

証明 この方程式は $X^4 + Y^4 = (Z^2)^2$ と書ける．これに定理 2 を適用すればよい． □

1.3 イデアルに関する補題と Euler の関数

$n \geq 1$ を自然数とする．n と互いに素な自然数 q で $0 \leq q \leq n$ となるものの個数を $\varphi(n)$ で表す．(0 と n は 互いに素でないから，$n > 1$ ならば $1 \leq q \leq n-1$ と書いても同じである．$\varphi(1) = 1$ とおく.) このように定められた関数 $\varphi(n)$ は **Euler の関数**とよばれる．もし p が素数ならば，明らかに，

$$\varphi(p) = p - 1. \tag{1}$$

$n = p^s$，素数 p のべきとすると，n と互いに素な整数は p の倍数でないものすべてとなる．1 と p^s の間には p の倍数は p^{s-1} 個ある．従って，

$$\varphi(p^s) = p^s - p^{s-1} = p^{s-1}(p-1). \tag{2}$$

さて，n が素数のべきの積として表されることを使って，$\varphi(n)$ を計算したい．この目的のために，$\varphi(n)$ のいくつかの性質とイデアルに関するいくつかの補題が必要である．これらの補題は後に用いられる．

命題 1. $n \geq 1$ を自然数とする．Euler の関数 $\varphi(n)$ の値は（巡回加法）群 $\mathbb{Z}/n\mathbb{Z}$ の生成元の個数に等しい．それはまた環 $\mathbb{Z}/n\mathbb{Z}$ の単元の個数とも等しい．

証明　$\bmod n\mathbb{Z}$ での各合同類は $0 \leq q \leq n-1$ をみたす唯 1 つの整数 q をそれぞれ含む．そのような整数 q に対して，$\overline{q}$ で $\bmod n\mathbb{Z}$ での剰余類を表すものとする．このとき，次のことを示せば十分である．すなわち，q は n と互いに素 $\Rightarrow$ $\overline{q}$ は $\mathbb{Z}/n\mathbb{Z}$ の中の単元 $\Rightarrow$ $\overline{q}$ は $\mathbb{Z}/n\mathbb{Z}$ を生成する $\Rightarrow$ q は n と互いに素である．q が n と互いに素であるとすると，Bezout の等式（1.1 節 (2)）より整数 x, y が存在して $qx + ny = 1$．よって $\overline{q} \cdot \overline{x} = \overline{1}$ が成り立ち，$\overline{q}$ は $\mathbb{Z}/n\mathbb{Z}$ で単元である．$\overline{q}$ を $\mathbb{Z}/n\mathbb{Z}$ で単元であるとする．x を整数として $\overline{q} \cdot \overline{x} = \overline{1}$ が成り立つから，任意の $\mathbb{Z}/n\mathbb{Z}$ の元 $\overline{a}$ $(0 \leq a < n)$ に対して，($\mathbb{Z}/n\mathbb{Z}$ において) $\overline{a} = \overline{a} \cdot \overline{x} \cdot \overline{q}$．従って（加法群 $\mathbb{Z}/n\mathbb{Z}$ において）$\overline{a} = (ax) \cdot \overline{q}$．ゆえに $\overline{q}$ は群 $\mathbb{Z}/n\mathbb{Z}$ を生成する．最後に，もし $\overline{q}$ が（加法群）$\mathbb{Z}/n\mathbb{Z}$ を生成するとすれば，ある $x \in \mathbb{Z}$ について $x \cdot \overline{q} = \overline{1}$ となり，$xq \equiv 1 \pmod{n}$ となるから，ある整数 y に対して $xq - 1 = yn$ が成り立つ．よって $1 = xq - yn$ となる．これは Bezout の等式の形であって，q は n と互いに素であることを示している．□

補題 1. A を環，$\mathfrak{a}$ と $\mathfrak{b}$ を A のイデアルで $\mathfrak{a} + \mathfrak{b} = A$ であるとする．このとき，$\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}$ で，標準的準同型 $\phi : A \to A/\mathfrak{a} \times A/\mathfrak{b}$ より同型 $\theta : A/\mathfrak{a}\mathfrak{b} \to A/\mathfrak{a} \times A/\mathfrak{b}$ を得る．

☞ 準同型 ϕ は $x \in A$ を x の $\bmod \mathfrak{a}$ での剰余類と x の $\bmod \mathfrak{b}$ での剰余類の組に写す写像である．

証明　一般に $\mathfrak{a}\mathfrak{b} \subset \mathfrak{a}$, $\mathfrak{a}\mathfrak{b} \subset \mathfrak{b}$ が成り立つから，$\mathfrak{a}\mathfrak{b} \subset \mathfrak{a} \cap \mathfrak{b}$ である．$x \in \mathfrak{a} \cap \mathfrak{b}$

とする．$\mathfrak{a}+\mathfrak{b}=A$ であるから元 $a\in\mathfrak{a}$ と $b\in\mathfrak{b}$ があって $a+b=1$ が成り立つ．よって $x=ax+bx$ は $\mathfrak{ab}$ の 2 つの元の和である．従って $x\in\mathfrak{ab}$ となり，$\mathfrak{a}\cap\mathfrak{b}\subset\mathfrak{ab}$ が示せた．ゆえに $\mathfrak{ab}=\mathfrak{a}\cap\mathfrak{b}$.

明らかに $\mathfrak{a}\cap\mathfrak{b}$ は ϕ の核である．$\mathfrak{a}\cap\mathfrak{b}=\mathfrak{ab}$ であることより，ϕ は mod $\mathfrak{ab}$ の各剰余類の上で不動である．よって，写像 $\theta: A/\mathfrak{ab}\to A/\mathfrak{a}\times A/\mathfrak{b}$ を得る．これは明らかに準同型である．$\phi^{-1}(0)=\mathfrak{ab}$ であることより，$\theta^{-1}(0)=(0)$ で θ は単射である．あとは θ が全射であることを示すことが残っている．

> ☞ 上の議論の中で,「剰余環に移って」といういい方をした．これからは同様な議論をより手短にこのようにいうことにする．

θ（同じことだが ϕ）が全射であることを示すのに，任意の $y\in A$, $z\in A$ に対してある元 $x\in A$ で $x+\mathfrak{a}=y+\mathfrak{a}, x+\mathfrak{b}=z+\mathfrak{b}$ が成り立つものを見つければよい．$a\in\mathfrak{a}$ と $b\in\mathfrak{b}$ を $a+b=1$ となるものとする．$x=az+by$ とおくと mod $\mathfrak{a}$ で $x\equiv by\equiv(1-a)y\equiv y-ay\equiv y$. 同様に $x\equiv z \bmod \mathfrak{b}$. □

補題 2. A を環とし，$(\mathfrak{a}_i)_{1\le i\le r}$ を A のイデアルの有限個の族で $\mathfrak{a}_i+\mathfrak{a}_j=A$ $(i\neq j)$ が成り立つものとする．このとき，$A/\mathfrak{a}_1\cdots\mathfrak{a}_r$ から $\prod_{i=1}^r A/\mathfrak{a}_i$ への標準的同型が存在する．

証明 補題 1 はこの補題で $r=2$ のときにあたる．r についての帰納法を用いる．$\mathfrak{b}=\mathfrak{a}_2\cdots\mathfrak{a}_r$ とおく．$\mathfrak{a}_1+\mathfrak{b}=A$ であることを示す．$i\ge 2$ に対して $\mathfrak{a}_1+\mathfrak{a}_i=A$ より元 $c_i\in\mathfrak{a}_1$ と $a_i\in\mathfrak{a}_i$ が存在して，

$$c_i+a_i=1,\qquad 1=\prod_{i=1}^{r}(c_i+a_i)=c+a_2\cdots a_n$$

となる．ここで，c は少なくとも 1 つの c_i を因子としてもつ項の和である．ゆえに，$c\in\mathfrak{a}_1$ である．$a_2\cdots a_r\in\mathfrak{b}$ であるから，$\mathfrak{a}_1+\mathfrak{b}=A$ となる．

補題 1 より，$A/\mathfrak{a}_1\mathfrak{b}$ は $A/\mathfrak{a}_1\times A/\mathfrak{b}$ と同型である．帰納法の仮定により，$A/\mathfrak{b}=A/\mathfrak{a}_2\cdots\mathfrak{a}_r$ は $A/\mathfrak{a}_2\times\cdots\times A/\mathfrak{a}_r$ に同型である．これらの同型を組み合わせれば，この補題が成り立つことがわかる． □

これらの補題を $\mathbb{Z}$ に適用してみよう.

命題 2. n と n' を互いに素な整数とする. このとき, $\mathbb{Z}/nn'\mathbb{Z}$ は環の直積 $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n'\mathbb{Z}$ に同型である.

証明 これは補題 1 の特別な場合である. 仮定より $n\mathbb{Z} + n'\mathbb{Z} = \mathbb{Z}$ (Bezout の等式) に注意する. □

系 1. n と n' が互いに素な正の整数とすれば, $\varphi(nn') = \varphi(n)\varphi(n')$ が成り立つ.

証明 $\varphi(nn')$ は環 $\mathbb{Z}/nn'\mathbb{Z}$ の単元の個数である (命題 1). $\mathbb{Z}/nn'\mathbb{Z}$ は $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n'\mathbb{Z}$ に同型である. さて, 元 $(\alpha, \beta) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n'\mathbb{Z}$ が可逆であることと, その各成分 α, β が可逆であることは同値である. よってこの系は命題 1 より得られる. □

系 2. n を正の整数で, $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ を素因数分解とする. このとき $\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right)$ が成り立つ.

証明 系 1 より $\varphi(n) = \varphi(p_1^{\alpha_1}) \cdots \varphi(p_r^{\alpha_r})$. 等式 (2) から $\varphi(p_i^{\alpha_i}) = p_i^{\alpha_i - 1}(p_i - 1) = p_i^{\alpha_i}\left(1 - \frac{1}{p_i}\right)$. これらを掛ければよい. □

1.4 加群についての準備

単項イデアル環上の加群を調べる前に, 一般の (可換) 環上の加群に言及しておこう.

A を (可換) 環, I を集合とする. I の元 i を添字とした A の元の列 $(a_i)_{i \in I}$ で, 有限個の $i \in I$ を除いて $a_i = 0$ であるようなものの集合を $A^{(I)}$ で表す. $A^{(I)}$ は直積 (cartesian product) 集合 A^I の部分集合になる. A^I に, 成分ごとに加法とスカラー倍で定義された A-加群の構造を入れたとき, $A^{(I)}$ は A^I の部分加群でもある.

もし I が有限であれば $A^{(I)} = A^I$ である.

δ_{ij} を $\delta_{jj}=1$ かつ $\delta_{ji}=0$ $(i\neq j)$ と定めたとき，任意の $j\in I$ に対して列 $(\delta_{ji})_{i\in I}$ は $A^{(I)}$ の元で，これを e_j と表す．$A^{(I)}$ のすべての元 $(a_j)_{j\in I}$ は $e_j(j\in I)$ の（有限個の）1 次結合として一意的に表される．より正確にいえば，

$$(a_j)_{j\in I}=\sum_{j\in I}a_je_j \tag{1}$$

（右辺の和においては，有限個を除いた項はすべて 0 であり，和は意味をなす）．

$(e_j)_{j\in I}$ を $A^{(I)}$ の**標準基底** (canonical basis) という．

A を環，M を A-加群，$\{x_i\}_{i\in I}$ を M の元の族とする．任意の $A^{(I)}$ の元 $(a_i)_{i\in I}$ に対して，M の元 $\sum_{i\in I}a_ix_i$ を関係づける（前と同じように，和は意味をなす）．これにより写像 $\phi: A^{(I)}\to M$ が得られる．これは線型である．$(e_i)_{i\in I}$ を $A^{(I)}$ の標準基底とするとき，すべての $i\in I$ に対して $\phi(e_i)=x_i$ である．次の主張がそれぞれ同値であることはすぐわかるであろう．

$$\{x_i\}_{i\in I}\text{が 1 次独立な集合である} \Longleftrightarrow \phi\text{が単射である．} \tag{2}$$

$$\{x_i\}_{i\in I}\text{が } M \text{ を生成する} \Leftrightarrow \phi\text{が全射である．} \tag{3}$$

もし ϕ が全単射のときは $\{x_i\}_{i\in I}$ を M の**基底** (basis) という．これは M の任意の元が $\{x_i\}_{i\in I}$ の 1 次結合として一意的に表されることを意味する．加群 M が基底をもつとき，**自由加群** (free module) といわれる．

☞ 体上のベクトル空間のときと違って，環上の加群は必ずしも基底をもつとは限らない．たとえば，$\mathbb{Z}$-加群 $\mathbb{Z}/n\mathbb{Z}$ $(n\neq 0,1)$．
後に，ある種の加群は自由であることを示す．この種の結果はそう自明なものではない．

有限な生成元の集合をもつとき，加群は**有限型** (finite type) といわれる．次の定理は Noether 環と加群の性質を調べる上で基礎となるものである．このトピックについてはさらに第 III 章で展開されるはずである．

定理 1. A を環，M を A-加群とする．次の条件は同値である．

(a) M の空でない任意の部分加群の族は（包含関係について）極大 (maximal) 元をもつ．

(b) M の部分加群の（包含関係による）増大列 $\{M_n\}_{n\geq 0}$ は静止する（すなわち，ある n_0 があって，任意の $n \geq n_0$ に対して $M_n = M_{n_0}$）．

(c) M の任意の部分加群は有限型である．

証明　(a) $\Rightarrow$ (b) を示す．E を M の部分加群，Φ を E の部分加群すべてからなる族とする．$(0) \in \Phi$ より Φ は空ではない．(a) によって Φ は極大元 F を含む．$x \in E$ に対して $F + Ax$ は E の部分加群で有限型である（これは $\{x\}$ と F の任意の生成元との和集合で生成される）．よって $F + Ax \supset F$ であるが，F が極大であることより $F + Ax = F$ となる．従って $x \in F, E \subset F, E = F$ となり，E は有限型である．

(c) $\Rightarrow$ (b) を示そう．$\{M_n\}_{n\geq 0}$ を M の部分加群の増大列とする．このとき $E = \bigcup_{n\geq 0} M_n$ は M の部分加群となる．(c) により，これは有限個の生成元 $\{x_1, \ldots, x_q\}$ をもつ．各 i に対して $n(i)$ があって $x_i \in M_{n(i)}$ となる．n_0 を $n(i)$ の中で最大のものとすれば，任意の i に対して $x_i \in M_{n_0}$ となり，$E \subset M_{n_0}$ なので $E = M_{n_0}$ となる．$n \geq n_0$ に対して包含関係 $M_{n_0} \subset M_n \subset E$ があることと $M_{n_0} = E$ から，$M_{n_0} = M_n$ を得る．ゆえに列 $\{M_n\}$ は n_0 を越えると静止する．

(b) $\Rightarrow$ (a) を示すことが残っている．ところで (a) と (b) が同値であることは次の半順序集合に関する補題の特別な場合である．

補題 1.　T を半順序集合 (partially ordered set) とする．次のことがらは同値である．

(a) T の任意の空でない部分集合は極大元を含む．

(b) 任意の T における増大列 $\{t_n\}_{n\geq 0}$ は静止する．

証明　(a) $\Rightarrow$ (b)　増大列 $\{t_n\}$ の極大元を t_q とする．このとき，$n \geq q$ に対して $t_n \geq t_q$（増大する），よって $t_n = t_q$（極大性より）．

(b) $\Rightarrow$ (a)　T の部分集合 S で極大元を含まないものがあったと仮定する．このとき，任意の $x \in S$ に対して，x より大きい S の元全体の集合は空ではない．選択公理により，写像 $f : S \to S$ で $f(x) > x$ がすべての $x \in S$ につ

いて成り立つものがある．S は空でないから，$t_0 \in S$ を選び，$t_{n+1} = f(t_n)$ とおくことにより列 $\{t_n\}_{n \geq 0}$ を帰納的に定義できる．これは真に増大する列で，静止しない．このことは (b) に矛盾する．よって (b) ⇒ (a) が示せた．□

定理 1 の系．単項イデアル環 A において，イデアルの任意の空でない族は極大元を含む．

証明　A を A 上の加群と考えると，その部分加群はイデアルである．すべてのイデアルが単項であることより，それらは唯 1 つの元で生成された A-加群である．よって有限型である．この系は定理 1 の (c) ⇒ (a) から得られる．□

1.5　単項イデアル環上の加群

A を整域，K をその分数体とする．自由 A-加群（ある I に対して $A^{(I)}$ と同型）は K 上のベクトル空間（$A^{(I)}$ においては $K^{(I)}$）の中に埋め込まれる．同様のことが自由 A-加群の任意の部分加群 M についても成り立つ．M で生成された部分空間の次元は M の**階数** (rank) といわれる．M 自身が自由であって n 個の基底をもつならば，M の階数は n である．

定理 1．A を単項イデアル環，M を階数 n の自由 A-加群とし，M' を M の部分加群とする．このとき，

(a) M' は階数 q $(0 \leq q \leq n)$ の自由加群である．

(b) もし $M' \neq (0)$ ならば，M の基底 $\{e_1, \ldots, e_n\}$ と 0 でない元 $a_1, \ldots, a_q \in A$ で，$\{a_1e_1, \ldots, a_qe_q\}$ が M' の基底となり a_i は a_{i+1} $(1 \leq i \leq q-1)$ を割り切るようなものがある．

証明　$M' = (0)$ のときは定理は明らかであるから，$M' \neq (0)$ とする．$L(M, A)$ は M における 1 次形式の集合を表す．$u \in L(M, A)$ に対して，$u(M')$ は A の部分加群，すなわち，イデアルである．イデアルは単項であるから $u(M') = Aa_u$ $(a_u \in A)$ と書いてよい．$u \in L(M, A)$ を Aa_u が Aa_v $(v \in L(M, A))$ の中で極大なものとする（1.4 節定理 1 の系）．M の基

底 $\{x_1,\ldots,x_n\}$ をとる．M は A^n と同一視される．$pr_i : M \to A$ を射影で i 番目の座標に写すもの，すなわち，$pr_i(x_j) = \delta_{ij}$ とする．$M' \neq (0)$ であることより，少なくとも 1 つの i $(1 \leq i \leq n)$ に対しては $pr_i(M') \neq (0)$. よって $a_u \neq 0$. 作り方より $e' \in M'$ が存在して $u(e') = a_u$ となる．任意の $v \in L(M,A)$ に対して，$a_u|v(e')$ であることを示そう．実際，もし $d = \mathrm{GCD}(a_u, v(e'))$ ならば $d = ba_u + cv(e')$ となる $b, c \in A$ がとれ，よって $d = (bu+cv)(e')$ となる．$bu+cv$ は M における 1 次形式であるから，$Aa_u \subset Ad \subset u(M')$ となる．Aa_u の極大性より $Ad = Aa_u$ となり，a_u は $v(e')$ を割り切る．

特に $a_u|pr_i(e')$ である．よって $pr_i(e') = a_u b_i$ $(b_i \in A)$ と表せる．$e = \sum_{i=1}^n b_i x_i$ とおくと，$e' = a_u e$ となる．$u(e') = a_u = a_u \cdot u(e)$ であるから $u(e) = 1$（ここで $a_u \neq 0$）．次のことを示そう．

(1) $M = \mathrm{Ker}(u) + Ae$,

(2) $M' = (M' \cap \mathrm{Ker}(u)) + Ae'$（ここで $e' = a_u e$），ここで和は直和である．

(1) の証明．任意の $x \in M$ に対して $x = u(x)e + (x - u(x)e)$ が成り立つ．$u(e) = 1$ であることより，$u(x - u(x)e) = u(x) - u(x)u(e) = 0$ となり，$x - u(x)e \in \mathrm{Ker}(u)$ を得る．これは $Ae + \mathrm{Ker}(u) = M$ を示している．明らかに $Ae \cap \mathrm{Ker}(u) = (0)$ である．

(2) の証明．$y \in M'$ に対して $u(y) = ba_u$ $(b \in A)$ と書ける．よって $y = ba_u e + (y - u(y)e) = be' + (y - u(y)e)$, $y - u(y)e \in \mathrm{Ker}(u)$ であることは容易にわかる．また $y - u(y)e = y - be' \in M'$. これより $y - u(y)e \in M' \cap \mathrm{Ker}(u)$ となり，(2) が示せた．

さて，階数 q についての帰納法で (a) を示す．もし $q = 0$ ならば $M' = (0)$ で何も示すことはない．$q > 0$ とする．$M' \cap \mathrm{Ker}(u)$ は (2) により階数 $q-1$ であり，従って帰納法の仮定により自由加群である．(2) において和は直和であったから，$M' \cap \mathrm{Ker}(u)$ の基底に e' を加えて，M の基底を得る．よって M' は自由加群であり，(a) が成り立つ．

(b) を示すために M の階数 n についての帰納法を用いる．$n = 0$ のと

きは自明である．(1) において和は直和であったから，(a) より $\mathrm{Ker}(u)$ は自由加群で階数 $n-1$ である．帰納法の仮定を自由加群 $\mathrm{Ker}(u)$ とその部分加群 $M' \cap \mathrm{Ker}(u)$ に適用する．すなわち，もし $M' \cap \mathrm{Ker}(u) \neq (0)$ ならば，$q \leq n$ と $\mathrm{Ker}(u)$ の基底 $\{e_2, \ldots, e_n\}$ と 0 でない $a_2, \ldots, a_q \in A$ が存在して，$\{a_2e_2, \ldots, a_qe_q\}$ が $M' \cap \mathrm{Ker}(u)$ の基底で a_i は a_{i+1} $(2 \leq i \leq q-1)$ を割り切る．上と同じ記号を用いて，$a_1 = a_u, e_1 = e$ とおく．このとき $\{e_1, \ldots, e_n\}$ は（(1) により）M の基底になり，$\{a_1e_1, \ldots, a_qe_q\}$ は（(2) と $e' = a_1e_1$ により）M' の基底になる．残るは $a_1|a_2$ を示すことである．v を M の 1 次形式で $v(e_1) = v(e_2) = 1, v(e_i) = 0$ $(i \geq 3)$ で定義されるものとする．このとき，$a_1 = a_u = v(a_ue_1) = v(e') \in v(M')$ となり，$Aa_u \subset v(M')$ を得る．Aa_u の極大性により，$v(M') = Aa_u = Aa_1$ となる．$a_2 = v(a_2e_2) \in v(M')$ であるから，$a_2 \in Aa_1$，すなわち，$a_1|a_2$ がいえる． □

☞ 定理 1 におけるイデアル Aa_i は M における M' の**不変因子** (invariant factor) とよばれる．それらは M と M' によって一意的に決まることが示せる（[1，第 VII 章，§3]）．

系 1. A を単項イデアル環，E を有限型の A-加群とする．このとき，E は直積 $(A/\mathfrak{a}_1) \times (A/\mathfrak{a}_2) \times \cdots \times (A/\mathfrak{a}_n)$ と同型になる．ここで，$\mathfrak{a}_i$ は A のイデアルで $\mathfrak{a}_1 \supset \mathfrak{a}_2 \supset \cdots \supset \mathfrak{a}_n$ をみたすものである．

証明 $\{x_1, \ldots, x_n\}$ を E の生成元の（有限）集合とする．1.4 節のはじめの部分によれば，全準同型 $\phi\colon A^n \to E$ で E が $A^n/\mathrm{Ker}(\phi)$ に同型となるものがある．定理 1 より，A^n の基底 $\{e_1, \ldots, e_n\}$ と，整数 $q \leq n$ と 0 でない元 $a_1, \ldots, a_q \in A$ があって，$\{a_1e_1, \ldots, a_qe_q\}$ が $\mathrm{Ker}(\varphi)$ の基底になり $a_i|a_{i+1}$ $(1 \leq i \leq q-1)$ をみたす．$q+1 \leq p \leq n$ に対しては $a_p = 0$ とおく．そうすると，$A^n/\mathrm{Ker}(\phi)$ は Ae_i/Aa_ie_i $(1 \leq i \leq n)$ の直積と同型になり，Ae_i/Aa_ie_i は A/Aa_i に同型である．$\mathfrak{a}_i = Aa_i$ とおけば，この系を得る． □

整域 A 上の加群 E は，もし $ax = 0$ $(a \in A, x \in E)$ ならば $a = 0$ または $x = 0$ が成り立つとき，**ねじれがない** (torsion-free) であるといわれる．

系 2. 単項イデアル環上において，ねじれがない有限型の加群は自由加群である．

証明　系 1 の記号を使う．$E \cong (A/\mathfrak{a}_1) \times \cdots \times (A/\mathfrak{a}_n)$．0 である部分は書かないことにして，$\mathfrak{a}_i \neq A$ $(1 \leq i \leq n)$ としてよい．$\mathfrak{a}_1 \neq (0)$ と仮定する．0 でない $a \in \mathfrak{a}_1$ をとり，$x_1 \in A/\mathfrak{a}_1$ を 0 でないものとする．$x = (x_1, 0, \ldots, 0)$ とおくと，$ax = 0$ となって，E がねじれがないことに矛盾する．従って $\mathfrak{a}_1 = (0)$．ところが $\mathfrak{a}_i \subset \mathfrak{a}_1$ であることより，任意の i に対して $\mathfrak{a}_i = (0)$ となる．よって E は A^n に同型になる．□

∞ E が有限型であることは本質的である．たとえば，$\mathbb{Q}$ はねじれのない $\mathbb{Z}$-加群であるが，自由加群ではない．

系 3. 単項イデアル環上において，任意の有限型加群 E は加群 M_i の有限直積と同型である．ここで M_i は A と等しいかまたは剰余加群 A/Ap^s（p は素元）に等しい．

証明　系 1 を用いて各部分 A/Aa $(a \neq 0)$ を 1.3 節の補題 2 によって分解する．もし $a = up_1^{s_1} \cdots p_r^{s_r}$ を a の素元分解とすれば，A/Aa は $A/Ap_i^{s_i}$ の直積と同型になる．□

系 4. G を有限可換群とする．このとき，G の元 x で，その位数が G のすべての元の位数の最小公倍数であるようなものが存在する．

証明　可換群は $\mathbb{Z}$-加群である（可換群を加法群と見る）．系 1 によれば，

$$G \cong \mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_n\mathbb{Z},$$

ここで $a_1|a_2|\cdots|a_n$．すべての i について $a_i \neq 0$（なぜなら，そうでないと G は無限群になるから）．1 の $\mathbb{Z}/a_n\mathbb{Z}$ での剰余類を y と表すとき，$x = (0, \ldots, 0, y)$ とおく．x の位数は明らかに a_n．任意の i に対して $a_i|a_n$ であるから，$z = (z_1, \ldots, z_n) \in G$ に対して $a_n z = 0$ となる．よって a_n は z の位数の倍数であり，x が探していた元である．□

1.6 体における 1 のべき根

定理 1. K を体とする．乗法群 $K^*(=K\setminus(0))$ の有限部分群は 1 のべき根からなり，巡回群である．

証明 1.5 節の定理 1 の系 4 によれば，ある $z\in G$ で，その位数を n とするとき，任意の元 $y\in G$ に対して $y^n=1$ が成り立つようなものがある．体上の次数 n の多項式（たとえば，X^n-1）は高々 n 個の根をその体の中でもつから，G の元の個数は高々 n 個である．さて，z は位数 n であるから G は n 個の元 $z,z^2,\dots,z^n=1$ を含み，それらはすべて異なる．よって G はこれらの元からなり，そして巡回群である． □

体 K が n 個の 1 の n 乗根を含めば，それらは位数 n の乗法的巡回群（加法群 $\mathbb{Z}/n\mathbb{Z}$ に同型）をなす．この群の生成元を 1 の**原始 n 乗根** (primitive n-th root of unity) という．任意の 1 の n 乗根は原始 n 乗根のべきで表される．1.3 節の命題 1 によれば，これら原始根の個数は $\varphi(n)$ 個である．

1.7 有限体

K を体とする．環の準同型 $\phi:\mathbb{Z}\to K$（$n\geq 0$ に対しては $\phi(n)=1+\cdots+1$（n 個），$\phi(-n)=-\phi(n)$ と定義する）が一意的に定められる．もし ϕ が単射であれば，それによって $\mathbb{Z}$ は K の部分環と同一視される．さらに $\mathbb{Z}$ の分数体 $\mathbb{Q}$ をも含むことになる．このとき，K は**標数** (characteristic) 0 であるという．もし ϕ が単射でないときは，その核はイデアル $p\mathbb{Z}$ $(p>0)$ であり，$\mathbb{Z}/p\mathbb{Z}$ は K の部分環と同一視できる．よって $\mathbb{Z}/p\mathbb{Z}$ は整域（実際は体）であり，p は素数である．この場合は，K は**標数** p であるという．ここから先では，$\mathbb{Z}/p\mathbb{Z}$ を $\mathbb{F}_p$ と表すことにする．

∞ K の部分体 $\mathbb{Q}$ または $\mathbb{F}_p$ は K の最小部分体であり，K の**素体** (prime field) といわれる．任意の素数 p に対して，標数 p の体，たとえば，$\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z}$ が存在する．

命題 1. K が標数 $p \neq 0$ の体ならば，任意の $x \in K$ について $px = 0$ となり，任意の x, $y \in K$ に対して $(x+y)^p = x^p + y^p$ が成り立つ．

証明 $x \in K$ に対して，$p \cdot x = (p \cdot 1) \cdot x = 0 \cdot x = 0$ となる．他方，二項定理より

$$(x+y)^p = x^p + y^p + \sum_{j=1}^{p-1} \binom{p}{j} x^j y^{p-j}.$$

二項係数 (binomial coefficient) $\binom{p}{j}$ は整数であり，それは $\frac{p!}{j!(p-j)!}$ に等しい．$1 \leq j \leq p-1$ のとき，素数 p はこの分子には現れるが分母には出てこないから，$\binom{p}{j}$ は p の倍数である．よって $(x+y)^p$ の展開における中間項は標数 p の体では消えてしまう． □

帰納的に考えれば，$(x+y)^{p^n} = x^{p^n} + y^{p^n}$ がすべての n に対して成り立つことがわかる．

定理 1. K を有限体とする．$q = \mathrm{card}(K)$ とする．このとき，

(a) K の標数は素数で，これを p とすれば，K は $\mathbb{F}_p$ 上の有限次元ベクトル空間であり，その次元を s とすれば，$q = p^s$ である．

(b) 乗法群 $K^*(= K \setminus (0))$ は位数 $q-1$ の巡回群である．

(c) 任意の $x \in K^*$ に対して $x^{q-1} = 1$ であり，任意の $x \in K$ に対して $x^q = x$ である．

証明 $\mathbb{Z}$ は有限でないから，K が標数 0 ではない．よって K は $\mathbb{F}_p$（p は素数）を含む．K は $\mathbb{F}_p$ 上のベクトル空間で，その次元 s は有限でなければならない．そうでないと，K は無限体になってしまう．ベクトル空間として K は $(\mathbb{F}_p)^s$ と同型であり，従って K は p^s 個の元を含む．(b) は 1.6 節の定理 1 からの帰結であり，(c) は (b) から容易に得られる． □

例. $\mathbb{F}_p$（p は素数）の場合について (b) を考えてみよう．整数 $x \in \mathbb{Z}$ $(0 < x \leq p-1)$ で，p の倍数でない任意の $y \in \mathbb{Z}$ が x のべきと法 p で合同になるようなものがある．そのような x は法 p の**原始根** (primitive root modulo p)

といわれる．法 p の原始根を見つける問題は決して自明ではない．たとえば，法 7 の原始根は $\varphi(6)=2$ 個で，3 と 5 である（$1^2 \equiv 6^2 \equiv 1 \pmod 7), 2^3 \equiv 4^3 \equiv 1 \pmod 7$ であり，3，5 はそれ以外の可能性をもつ唯一のものである）．

注意. (a) と (c) より，q 個の元からなる有限体 K は多項式 $X^q - X$（これは q 個の根しかもたない）の根全体の集合である．q 個の元からなる 2 つの有限体は同型になることを示すことができる．q 個の元からなる体を $\mathbb{F}_q$ と表すことにする．

演習として有限体上の Diophantus 方程式に関連する次のエレガントな定理を証明するため，話をわき道にそれる．

定理 2 (Chevalley). K を有限体，$F(X_1, \ldots, X_n)$ を K 上の次数 d の斉次多項式とする．$d < n$ とすれば，点 $(x_1, \ldots, x_n) \in K^n \setminus (0)$ があって，$F(x_1, \ldots, x_n) = 0$ となる．

☞ K を体，j を整数とし，次数 d で変数 n 個 $(n > d^j)$ の任意の斉次多項式が $K^n \setminus (0)$ で 0 の値をとるとき，K は C_j-体であるという．C_0-体は代数的閉体である．Chevalley の定理は有限体は C_1-体（これを「準代数的閉体」(quasi-algebraically closed) ともいう）であることをいっている．もし K が C_j-体であれば K の 1 変数の有理関数体 $K(t)$ と 1 変数の形式的べき級数体 $K((t))$ は C_{j+1}-体である（[5]）．p-進体が C_2-体であるかどうかということは長い間未解決であった．最近，そうでないということが示された（[8]）．

定理 2 の証明　$q = \mathrm{card}(K)$ とおき，p を K の標数とする（$q = p^s$ と書ける）．$V \subset K^n$ を F を 0 にするものの集合とする．すなわち，点 $(x_1, \ldots, x_n) \in K^n$ で $F(x_1, \ldots, x_n) = 0$ をみたすもの全体の集合である．(今後，$(x_1, \ldots, x_n) \in K^n$ を x と表す.) 定理 1(c) より，$F(x)^{q-1} = 0$ $(x \in V)$ かつ $F(x)^{q-1} = 1$ $(x \in K^n \setminus V)$ である．よって多項式 $G(X) = F(X)^{q-1}$ は値を $\mathbb{F}_p$ にもつ $K^n \setminus V$ の特性関数 (characteristic function) である．従って，$K^n \setminus V$ の点の法 p での個数は和 $\sum_{x \in K^n} G(x)$ で与えられる．この和を計算して，それが 0 であることを示せばよい．実際これが示せたとしよう．

すると $\mathrm{card}(K^n \setminus V)$ は p の倍数であり，$\mathrm{card}(K^n) = q^n = p^{ns}$ は p の倍数であるから $\mathrm{card}(V)$ は p の倍数でなければならない．明らかに V は原点を含む．$p|\mathrm{card}(V)$ であることより V は必然的に他の点を含む（$p \geq 2$）．よって，定理 2 を証明するには $\sum_{x\in K^n} G(x) = 0 \in \mathbb{F}_p$ を示せばよい．さて，$\sum_{x\in K^n} G(x)$ を計算しよう．多項式 G は単項式 $M_\alpha(X) = X_1^{\alpha_1}\cdots X_n^{\alpha_n}$ の 1 次結合である．$\sum_{x\in K^n} G(x)$ を決定するためには $\sum_{x\in K^n} M_\alpha(x) = \sum_{x\in K^n} x_1^{\alpha_1}\cdots x_n^{\alpha_n} = (\sum_{x_1\in K} x_1^{\alpha_1})\cdots(\sum_{x_n\in K} x_n^{\alpha_n})$ を計算すれば十分である．よって問題は $\sum_{z\in K} z^\beta$ ($\beta \in \mathbb{N}$) の形の和を計算することに帰着する．

(a) $\beta = 0$ のときは，任意の $z \in K$ に対して $z^\beta = 1$．結局 $\sum_{z\in K} z^\beta = \sum_{z\in K} 1 = q = 0$.

(b) $\beta > 0$ のとき，項 $0^\beta = 0$ であるから和は $\sum_{z\in K^*} z^\beta$ に等しい．ところで，K^* は巡回群で位数 $q-1$（定理 1(b)）である．ω を K^* の生成元とするとき，$\sum_{z\in K^*} z^\beta = \sum_{j=0}^{q-2} \omega^{\beta j}$ となる．これは等比数列の和になる．よって，

(b′) $\omega^\beta \neq 1$ ならば，すなわち，β が $q-1$ の倍数でないならば，

$$\sum_{j=0}^{q-2} \omega^{\beta j} = \frac{\omega^{\beta(q-1)} - 1}{\omega^\beta - 1} = 0$$

となる．なぜならば，$\omega^{q-1} = 1$ だからである．

(b″) $\omega^\beta = 1$，すなわち，β が $q-1$ の倍数ならば，

$$\sum_{j=0}^{q-2} \omega^{\beta j} = q - 1$$

となる．

(a)，(b′) と (b″) より，$\sum_{x\in K^n} x_1^{\alpha_1}\cdots x_n^{\alpha_n}$ はすべての α_i が 0 でなくかつ $q-1$ の倍数でもない場合を除き，0 となる．このとき単項式の次数は $\alpha_1 + \cdots + \alpha_n \geq (q-1)n$ である．ところが，$G = F^{q-1}$ であることより，G は次数 $(q-1)d$ をもち，仮定より $(q-1)d < (q-1)n$．ゆえに，G に現れる 0 係数でないすべての単項式 $M_\alpha(X)$ に対して $\sum_{x\in K^n} M_\alpha(x) = 0$ が成り立つ．従って，$\sum_{x\in K^n} G(x) = 0$．これで結論を得た．　□

∞ F が斉次であるという代わりに，F が定数項をもたないということで十分である．次数と変数の個数との間の不等式 $d < n$ は本質的である．たとえば，$\mathbb{F}_{q^n}$ の $\mathbb{F}_q$ へのノルム（2.6 節を参照）は次数 n の n 変数の斉次多項式であって，それを 0 にする自明でない解がある．

例．有限体上の 3 変数の 2 次形式は 0 になり得る（すなわち，値が 0 になるような自明でない解をもつ）．K^3 から射影平面 $\mathbb{P}_2(K)$ に移ることによって，これは K 上の 2 次曲線が K 上の有理点をもつ（すなわち，その座標が K の中でとれる）ことを意味する．$\mathbb{R}$ 上の 2 次曲線 $X^2 + Y^2 + Z^2 = 0$ の例（あるいは，$\mathbb{Q}$ 上の $X^2 + Y^2 - 3Z^2 = 0$ である．これが $\mathbb{Q}$ 上自明でない解をもたないことを示すには，x, y, z が互いに素な整数の場合を考えればよく，その結果，法 4 のときに還元される）は，定理 2 がすべての体に共通する性質を扱っているのではないことを示している．

練習問題

1*. p を素数とし，$r \in \mathbb{N}$ とする．乗法群 $(\mathbb{Z}/p^r\mathbb{Z})^*$ は，$p=2$ かつ $r \geq 3$ の場合を除いて，巡回群であることを示せ（ヒント：p が奇数のとき，$1+p$ の $\mathbb{Z}/p^r\mathbb{Z}$ の中の剰余類は位数 p^{r-1} であることを示す．$p=2$ については，5 の剰余類の位数を考える．そして 1.5 節の定理 1 の系 4 を用いる）．

2*. (a) Diophantus 方程式 $X^2+Y^2=3Z^2$ は自明でない整数解（すなわち，$\neq (0,0,0)$）をもたないことを示せ（ヒント：法 3 で簡約する）．また，$X^2+Y^2=7Z^2$ と $X^2+Y^2=11Z^2$ についても同様であることを示せ．
(b) $X^2+Y^2=5Z^2$ と $X^2+Y^2=13Z^2$ は自明でない整数解をもつことを示せ．
(c) p を素数とするとき，(a) を $X^2+Y^2=pZ^2$ の方程式に一般化せよ（ヒント：このような条件の下で -1 が $\mathbb{F}_p^*$ において平方になるか調べる）．

3*. 素数が無限に存在することの古典的証明を再発見せよ．類似の方法で，$4k-1$ ($k \in \mathbb{N}$) の形の素数が無限個あることを示せ．

4*. $n \in \mathbb{N}$ が素数であるためには n が $(n-1)!+1$ を割り切ることが必要十分であることを示せ（ヒント：n が素数のときは $\mathbb{F}_n^*$ のすべての元の積を計算する．n が素数でないときは，どんなことが起きるかチェックする）．

5*. 有限体 K においては，すべての元は 2 つの平方の和であることを示せ（ヒント：最初に $q=\mathrm{card}(K)$ が偶数のときを扱い，q が奇数のとき，$a \in K$ を固定して関数 $x \mapsto x^2, y \mapsto a-y^2$ $(x,y \in K)$ の値の個数を計算する）．

6*. 多項式 X^3-X+1 を $\mathbb{F}_{23}$ において，X^3+X+1 を $\mathbb{F}_{31}$ において，因数分解せよ（ヒント：それぞれは 2 重根と単根をもつ）．

7. 環 A の 2 つのイデアル $\mathfrak{a},\mathfrak{b}$ で，$\mathfrak{a}\cap\mathfrak{b} \neq \mathfrak{a}\mathfrak{b}$ である例をあげよ．$\mathfrak{a}\cdot\mathfrak{b} \subset \mathfrak{a}\cap\mathfrak{b}$ は常に成り立つことを示せ．

8*. A を整域とし，$a,b \in A$，$B=A[X]/(aX+b)$ とする．$Aa \cap Ab = Aab$ ならば B は整域であることを示せ（ヒント：K を A の分数体として，元 $-b/a \in K$ を考え，準同型 $\varphi: A[X] \to K$ を $\varphi(X)=-b/a$, $\varphi(y)=y$ $(y \in A)$ と定義して，これの核が $(aX+b)$ であることを示す）．

9*. A を整域，i と j を互いに素な整数とする．多項式環 $A[X,Y]$ のイデアル (X^i-Y^j) は素イデアルであることを示せ（ヒント：準同型 $A[X,Y] \to A[X]$ で核

がそのイデアルになるものを考える）．

10*． (a) A を整域，K をその分数体，a, b を A の 0 でない元とする．A-加群 $\mathrm{Hom}(A/bA, K/A)$ は A/bA と同型であることを示せ（ヒント：A-加群 E, F について，$\mathrm{Hom}(E, F)$ は E から F への準同型，ないしは A-線型写像の集合を表していた．$\mathrm{Hom}(E, F)$ は A-加群である．準同型 $\phi: A/bA \to K/A$ は 1 の剰余類のそれによる値で定まることに注意する）．

(b) A-加群 E に対して $E' = \mathrm{Hom}(E, K/A)$，$E'' = \mathrm{Hom}(E', K/A)$ とおく．標準的な準同型 $E \to E''$ を定義せよ．

(c) A を単項イデアル環とする．E を A 上の有限型のねじれ (torsion) 加群（すなわち，任意の $x \in E$ に対して，ある $a \in A \setminus (0)$ が存在して，$ax = 0$）とする．E の構造を決定し，(a) から E は $E' = \mathrm{Hom}(E, K/A)$ に同型であることを示し，これより標準的準同型 $E \to E''$ は同型であることを導け．

第 II 章　環上の整元，体上の代数的元

複素数の中で本書に関係するものは，いわゆる**代数的数** (algebraic number) である．これは有理数を係数とする次の形の方程式

$$X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 = 0$$

をみたす元である．係数が整数 ($a_i \in \mathbb{Z}$) であるときは，代数的数 x は**代数的整数** (algebraic integer) といわれる．従って，$\sqrt{2}$, $\sqrt{3}$, i, $e^{2i\pi/5}$ は代数的整数である．代数的数（あるいは，代数的整数）の和や積がまた代数的数（あるいは，代数的整数）になることは先天的に明らかなことではない．たとえば，$x = \sqrt{2} + \sqrt{3}$ を考える．両辺を平方して $x^2 = 2 + 3 + 2\sqrt{6}$ を得て，加算と移項をすることにより $x^2 - 5 = 2\sqrt{6}$ となり，再度平方して $(x^2-5)^2 = 24$ を得る．これにより x は代数的整数であることがわかる．読者は $\sqrt[3]{5} + \sqrt[5]{7}$ が代数的整数であることを示してみるとよい．この数が代数的であることを示すに至るための一連の段階は容易には一般化されるものではないということを確信するであろう．

この困難を打破するために，前世紀の代数学者たち，特に Dedekind，は問題を「線型化」するというアイディアをもった．つまり，彼らが加群の概念を導入したということである．ここでは加群に関するいくつかの結果から始めることにしよう．$\mathbb{Z}$（あるいは $\mathbb{Q}$）の代わりに可換環上の加群を考えることは何ら労を加える必要がないし，後に非常に有益になることであろう．まず環上の整元の一般論からはじめ，その後体上の代数的元に専念することにする．

2.1 環上の整元

定理 1. R を環，A を R の部分環，x を R の元とする．次のことがらは同値である．

(a) ある $a_0, \ldots, a_{n-1} \in A$ が存在して，

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0 \tag{1}$$

が成り立つ．(すなわち，x は A に係数をもつ最高次数の係数が 1 である多項式の解である．)

(b) 環 $A[x]$ は有限型の A-加群である．

(c) R の部分環 B で A と x を含み，かつ有限型の A-加群であるものが存在する．

証明 M を $1, x, \ldots, x^{n-1}$ で生成される R の部分 A-加群とする．(a) により，$x^n \in M$．(1) に x^j を掛けることにより，$x^{n+j} = -a_{n-1}x^{n+j-1} - \cdots - a_0 x^j$ を得る．実際問題として，j についての帰納法で $x^{n+j} \in M$ が任意の $j \geq 0$ について成り立つことが示せる．$A[x]$ は x^k $(k \geq 0)$ 全体で生成される A-加群であるから，$A[x] = M$ となる．よって (a) より (b) がいえた．(b) から (c) が出ることは明らか．(c) から (a) がいえることを示す．$\{y_1, \ldots, y_n\}$ を B の A-加群としての生成元の有限集合とする．すなわち，$B = Ay_1 + \cdots + Ay_n$ である．$x \in B$ で B は R の部分環であることより，$xy_i \in B$ がすべての $i = 1, \ldots, n$ について成り立つ．よって，

$$xy_i = \sum_{j=1}^{n} a_{ij} y_j \qquad (i = 1, \ldots, n, \ \ a_{ij} \in A, \ 1 \leq i, j \leq n)$$

と表される．これより，

$$\sum_{j=1}^{n} (\delta_{ij} x - a_{ij}) y_j = 0 \qquad (i = 1, \ldots, n)$$

を得る．この $\{y_1, \ldots, y_n\}$ についての n 個の 1 次方程式を考える．行列式 $\det(\delta_{ij} x - a_{ij})$ を d と表す．Cramer の方法によりすべての i に対して

$dy_i = 0$ となる．これは任意の $b \in B = \sum_i Ay_i$ に対して $db = 0$ となることを意味し，特に $d = d \cdot 1 = 0$ を得る．しかし，d は明らかに x についての最高次数の係数が 1 である多項式で表される．なぜならば，最高次の項は主対角成分の積 $\prod_{i=1}^{n}(x - a_{ii})$ の展開の中に現れるからである．従って (c) より (a) が導かれる．□

定義 1. R を環，A を R の部分環とする．R の元 x は，定理 1 の同値条件 (a)，(b)，(c) をみたすとき，A **上整** (integral) であるといわれる．$P(X) \in A[X]$ を最高次の係数が 1 の多項式で $P(x) = 0$ となるものとする（(a) はこのような多項式の存在を示している）．関係 $P(x) = 0$ は x の A 上の**整従属** (integral dependence) の方程式とよばれる．

☞ **例.** $\mathbb{R}$ の元 $x = \sqrt{2}$ は $\mathbb{Z}$ 上整である．関係 $x^2 - 2 = 0$ が整従属の方程式である．

命題 1. R を環，A を R の部分環，$\{x_i\}_{1 \le i \le n}$ を R の有限部分集合とする．すべての i について，x_i が $A[x_1, \ldots, x_{i-1}]$ 上整（特にすべての x_i が A 上整）ならば，$A[x_1, \ldots, x_n]$ は有限型の A-加群である．

証明　n についての帰納法を用いる．$n = 1$ のときは定理 1(b) の繰り返しである．命題が $n-1$ まで正しいと仮定する．すなわち，$B = A[x_1, \ldots, x_{n-1}]$ が有限型の A-加群であると仮定する．このとき $B = \sum_{j=1}^{p} Ab_j$ と書ける．$n = 1$ の場合により $A[x_1, \ldots, x_n] = B[x_n]$ は有限型の B-加群である．$B[x_n] = \sum_{k=1}^{q} Bc_k$ と表す．このとき，

$$A[x_1, \ldots, x_n] = \sum_{k=1}^{q} Bc_k = \sum_{k=1}^{q}(\sum_{j=1}^{p} Ab_j)c_k = \sum_{j,k} Ab_jc_k$$

となる．よって $\{b_jc_k\}_{1 \le j \le p, 1 \le k \le q}$ は A-加群としての $A[x_1, \ldots, x_n]$ の生成元の有限集合である．□

系 1. R を環，A を R の部分環，x と y を A 上整な R の元とする．このとき，$x + y$，$x - y$，xy は A 上整である．

証明　明らかに $x+y$, $x-y$, $xy \in A[x,y]$ である．命題 1 により，$A[x,y]$ は有限型の A-加群である．定理 1 の (c) によって，$x+y$, $x-y$, xy は A 上整である．□

系 2. R を環，A を R の部分環とする．R の元で A 上整であるもの全体の集合を A' と表すとき，A' は R の部分環で A を含むものになる．

証明　系 1 は A' が R の部分環であることを示している．任意の $a \in A$ は A に係数をもつ最高次の係数が 1 の多項式 $P(X) = X - a$ の根であるから，$A \subset A'$ である．□

定義 2. R を環，A を R の部分環とする．A 上整である R の元のなす環 A' は A の R における**整閉包** (integral closure) とよばれる．A が整域で K がその分数体とするとき，A の K における整閉包を A の**整閉包**という．B を環で A を B の部分環とするとき，B が A 上整であるというのは，任意の B の元が A 上整であるとき（すなわち，A の B における整閉包が B 自身であること）である．

命題 2（推移律）. C が環，B が C の部分環，A が B の部分環とする．もし，B が A 上整で C は B 上整であれば，C は A 上整である．

証明　$x \in C$ をとると，x は B 上整であり，x は整従属の方程式 $x^n + b_{n-1}x^{n-1} + \cdots + b_0 = 0$ $(b_i \in B)$ をもつ．$B' = A[b_0, \ldots, b_{n-1}]$ とおく．このとき，x は B' 上整である．B は A 上整であるから，すべての b_i は A 上整である．よって，命題 1 により $B'[x] = A[b_0, \ldots, b_{n-1}, x]$ は有限型の A-加群である．定理 1 の (c) によって，x は A 上整となる．ゆえに C は A 上整である．□

命題 3. B を整域とし，A は B の部分環で B が A 上整となるものとする．このとき，B が体であることと A が体であることは同値である．

証明　A が体であるとする．$b \in B, b \neq 0$ をとる．このとき，$A[b]$ は A 上有限次元のベクトル空間（定理 1 の (b)）である．他方，$y \mapsto by$ は $A[b]$ の A-

線型写像であり，$A[b]$ が整域で $b \neq 0$ であるから，これは単射である．従って，これは全射になる．ある $b' \in A[b]$ があって，$bb' = 1$ となる．このことは，任意の $b \in B \setminus (0)$ が B において可逆であることを意味する．よって B は体*である．

逆に，B が体であるとする．$a \in A \setminus (0)$ をとる．このとき a は逆元 $a^{-1} \in B$ をもち，それは整従属の方程式

$$a^{-n} + a_{n-1}a^{-n+1} + \cdots + a_1 a^{-1} + a_0 = 0 \quad (a_i \in A)$$

をみたす．a^{n-1} を掛けることにより，

$$a^{-1} = -(a_{n-1} + \cdots + a_1 a^{n-2} + a_0 a^{n-1})$$

を得る．これは $a^{-1} \in A$ を示している．ゆえに A は体である．　□

2.2　整閉環

定義．環 A は，整域であって A 自身がそれ上の整閉包であるとき，**整閉** (integrally closed) であるといわれる．言い換えると，A の分数体 K の任意の元 x が A 上整であれば $x \in A$ となる，ということである．

例 1. A を整域，K を A の分数体とする．このとき A の整閉包 A'（すなわち K における A の整閉包）は整閉である．実際，A' の整閉包は A' 上整であり，従って A 上整である（2.1 節命題 2）．よって A' に一致する．

例 2. すべての単項イデアル環は整閉である．

証明　定義よりすべての単項イデアル環は整域である．x を A の分数体の元で A 上整であるものとする．

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0 \quad (a_i \in A) \tag{1}$$

を x の A 上の整従属の方程式とする．$a, b \in A$ を互いに素なものにとって

* 写像 $y \mapsto by$ を考えることにより，同じ理由で，有限な整域は体であることが示せる．

$x = a/b$ と書ける．(1) に代入して b^n を掛けて，

$$a^n + b(a_{n-1}a^{n-1} + \cdots + a_1ab^{n-2} + a_0b^{n-1}) = 0$$

を得る．よって b は a^n を割り切る．b と a は互いに素であるから，Euclid の補題を繰り返し用いて，b は a を割り切ることが示される．従って，b は A の単元である．よって $x = a/b \in A$ となり，A は整閉であることが示せた．　□

☞ 単項イデアル環の乗法的性質（互いに素，Euclid の補題）のみが使われていることがわかると思う．同じ議論によって，すべての一意分解環が整閉であることが示される．

2.3　体上の代数的元，代数拡大

定義．R を環，K を R の部分体とする．元 $a_0, \ldots, a_n \in K$（少なくとも 1 つは 0 でない）があって，$a_nx^n + \cdots + a_1x + a_0 = 0$ が成り立つような元 $x \in R$ は K 上**代数的** (algebraic) であるといわれる．

言い換えると，いくつかの単項式 $\{x^j\}_{j\in\mathbb{N}}$ が K 上 1 次従属であることである．K 上代数的でない R の元は K 上**超越的** (transcendental) とよばれ，すなわち，x が K 上超越的であることと，$\{x^j\}_{j\in\mathbb{N}}$ が K 上 1 次独立であることは同値である．

定義の関係式において $a_n \neq 0$ と仮定してよい．このとき，$a_n^{-1} \in K$ で，a_n^{-1} を掛けることにより整従属の方程式が得られる．従って

$$\text{体上においては,「代数的」=「整」となる.} \tag{1}$$

よって整元についてのことがらを適用できる．たとえば，$K \subset R$ で $x \in R$ に対して，2.1 節の定理 1(b) より

$$x \text{ は } K \text{ 上代数的} \Leftrightarrow [K[x] : K] \text{ は有限.} \tag{2}$$

体 K を含む環 R の任意の元が K 上代数的のとき，R は K 上**代数的** (algebraic) であるという．R が体のときは，R は K 上の**代数拡大** (algebraic

extension) といわれる．

体 L とその部分体 K に対して，次元 $[L:K]$ を K 上の**次数** (degree) という．この流れでいくと，2.1 節の定理 1(c) は次のようにいえる，すなわち

$$L \text{ の } K \text{ 上の次数が有限であれば, } L \text{ は } K \text{ の代数拡大である．} \tag{3}$$

$\mathbb{Q}$ 上の有限次数の拡大は**代数体** (algebraic number field)（あるいは単に，**数体** (number field)）といわれる．

命題 1. K を体，L を K の代数拡大，M を L の代数拡大とする．このとき，M は K の代数拡大である．さらに $[M:K]=[M:L][L:K]$（次数の乗法性）が成り立つ．

証明　第 1 の主張は 2.1 節の命題 2 の特殊な場合である．さらに，$\{x_i\}_{i\in I}$ を L の K 上の基底，$\{y_j\}_{j\in J}$ を M の L 上の基底とすれば，$\{x_iy_j\}_{(i,j)\in I\times J}$ は 2.1 節の命題 1 と同様にして，K 上 M を生成することがわかる．関係 $\sum_{i,j} a_{ij}x_iy_j = 0$ $(a_{ij}\in K)$ は $\sum_j(\sum_i a_{ij}x_i)y_j = 0$ と書けて，すべての j について $\sum_i a_{ij}x_i = 0$ となる（$\sum a_{ij}x_i \in L$ に注意する）．ゆえに，すべての $(i,j)\in I\times J$ について $a_{ij}=0$ となる．これは $[M:K]=[M:L][L:K]$ を示している．□

命題 2. R を環，K を R の部分体とする．このとき，

(a) K 上代数的な R の元全体の集合 K' は K を含む R の部分環である．

(b) R が整域ならば，K' は R の部分体になる．

証明　(a) は 2.1 節命題 1 の系 2 の特殊な場合にあたる．(b) は 2.1 節命題 3 による．□

さて，体上の代数的元についてより細かく調べることにしよう．R を環，K を R の部分体，X を R の元とする．$K[X]$ は K 上 1 変数の多項式環を表す．準同型 $\phi: K[X]\to R$ を $\phi(X)=x$，$\phi(a)=a$ $(a\in K)$ とすること

で一意的に与えることができる．ϕ の像は $K[x]$ である．代数的元は次のように再定義できる．

$$元\ x\ は\ K\ 上代数的 \Leftrightarrow \mathrm{Ker}(\phi) \neq (0). \tag{4}$$

実際，もし x が K 上超越的であれば，$\mathrm{Ker}(\phi) = (0)$ であることは明らかである．ともかく，イデアル $\mathrm{Ker}(\phi)$ は単項イデアル $(F(X))$ である（$K[X]$ は単項イデアル環であるから）．x が K 上代数的のときは，$\mathrm{Ker}(\phi)$ は 0 でない多項式 $F(X)$ で生成される．

K は体であるから $F(X)$ は最高次の係数は 1 としてよい．$F(X)$ は K と x で一意的に定まる．$F(X)$ を x の K 上の**最小多項式** (minimal polynomial) という．最小多項式は次のような性質をもつ．すなわち，$F(X)$ を x の K 上の最小多項式とする．$G(X) \in K[X]$ に対して，

$$G(x) = 0 \;\Leftrightarrow\; K[X]\ において\ G(X)\ は\ F(X)\ で割り切れる. \tag{5}$$

剰余環に移行して，**標準的同型** (canonical isomorphism)

$$K[X]/(F(X)) \;\tilde{\rightarrow}\; K[x] \tag{6}$$

を得る．

同じ記号の下で，今度は x が K 上代数的とし，$F(X)$ をその最小多項式とする．(5) と 2.1 節の命題 3 より，次の同値な条件を得る．

$$K[x]\ は体 \Leftrightarrow K[x]\ は整域 \Leftrightarrow F(X)\ は既約. \tag{7}$$

他方，K が体で $F(X) \in K[X]$ が既約ならば，$K[X]/(F(X))$ は K を含む体である．$X \in K[X]$ のこの体への射影を x と書けば，$F(x) = 0$ となる．よって $X - x$ は $K[X]$ において $F(X)$ を割り切る．より一般的には次が成り立つ．

命題 3. K を体，$P(X) \in K[X]$ を定数でない多項式とする．このとき，K の有限次代数拡大 K' で，$P(X)$ は $K'[X]$ において次数 1 の多項式（線型多項式）の積に分解するようなものが存在する．

証明　$P(X)$ の次数 d についての帰納法を用いる．$d = 1$ のときは証明すべき

ものは何もない．次数 $d-1$ のときには主張が証明されたと仮定する．$F(X)$ を $P(X)$ の既約因子とする．K の有限次拡大 K''（たとえば，$K[X]/(F(X))$）で，元 x を含み，$K''[X]$ で $X-x$ が $F(X)$ を割り切るようなものがあることは今まで見てきた通りである．よって $P(X)=(X-x)P_1(X)$ $(P_1(X)\in K''[X])$ と書ける．帰納法の仮定により，K'' の有限次拡大 K' をとれば $K'[X]$ において $P_1(X)$ は線型多項式の積に分解する．命題 1 により，K' は K 上有限次数であり，$P(X)$ は $K'[X]$ において線型多項式の積になる．　□

注意．代数的閉体． 体 K は，定数でないすべての多項式 $P(X)\in K[X]$ が $K[X]$ において線型多項式の積として表されるとき，**代数的に閉じている** (algebraically closed) といわれる．そうであることを示すには，多項式の次数についての帰納法によって定数でないすべての多項式が K において根をもつことを示せば十分である．命題 3 を Zorn の補題（[1，第 V 章]，[9，第 II 章] を参照）によって拡張すれば，任意の体は代数的閉体に埋め込むことができることが示される．

解析学の手法を用いた多くの異なる方法†により，複素数体 $\mathbb{C}$ は代数的閉体であることが証明される．これ以上多くは必要ないであろう．

2.4　共役元，共役体

体 K を含む 2 つの体 L と L' が与えられたとき，同型 $\phi: L\to L'$ であって任意の $a\in K$ に対して $\phi(a)=a$ となるものを L から L' の上への **K-同型** (K-isomorphism) という．このとき，L と L' は **K-同型** (K-isomorphic) ないしは（それらが K 上代数的のとき）K 上**共役** (conjugate) であるという．K の 2 つの拡大体 L と L' があるとき，$x\in L$ と $x'\in L'$ について，ある K-同型 $\phi: K(x)\to K(x')$ があって $\phi(x)=x'$ のとき，x と x' は K 上**共役** (conjugate) であるという．そのような ϕ はもちろん一意的に決まる．

† コンパクト位相空間上に定義される連続関数の性質に依存する証明については [4] を参照．複素変数の解析関数の性質を用いる証明については [3] を参照．後に，この章の付録として，より代数的な証明を与えるつもりである．それは実数についての最も初等的な性質を越えるような解析は含まないはずである．

ϕ が存在するということは x と x' がともに K 上超越的であるかまたは K 上代数的で同じ最小多項式をもつことを意味する（2.3 節 (5) を参照）．

例． $F(X)$ を K 上 n 次の既約多項式，$x_1, \ldots, x_n$ を K の拡大体 K' における $F(X)$ の根とする（2.3 節命題 3）．このとき $x_1, \ldots, x_n$ はどの 2 つも K 上共役であり（2.3 節 (6)），$K[x_1], \ldots, K[x_n]$ のどの 2 つも共役である．

補題． K を標数 0 の体または有限体，$F(X) \in K[X]$ を最高次の係数が 1 の既約多項式であって，$F(X) = \prod_{i=1}^{n}(X - x_i)$ を K の拡大体 K' における線型多項式の積への分解とする（2.3 節命題 3）．このとき，$F(X)$ の n 個の根 $x_1, \ldots, x_n$ はすべて異なる．

証明　結論が成り立たないとすると，$F(X)$ はその導関数 $F'(X)$ と共通根をもつ．よって $F(X)$ は $F'(X)$ を割り切る（2.3 節 (4)）．$\deg(F'(X)) < \deg(F(X))$ であるから，$F'(X)$ は多項式として 0 である．ところが，$F(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ $(a_i \in K)$ とおくと，

$$F'(X) = nX^{n-1} + (n-1)a_{n-1}X^{n-2} + \cdots + a_1$$

である．よって $n \cdot 1 = 0$, $j \cdot a_j = 0$ $(j = 1, \ldots, n-1)$ となり，標数が 0 であるときはこれは不可能である．

標数 $p \neq 0$ のときは，これより p は n を割り切り，p で割り切れない j に対しては $a_j = 0$ となる（ここで p は素数であった）．よって $F(X)$ は

$$F(X) = X^{qp} + b_{q-1}X^{(q-1)p} + \cdots + b_1X^p + b_0 \quad (b_i \in K)$$

の形となる．もし，各 b_i が p 乗，すなわち，$b_i = c_i^p$ $(c_i \in K)$ ならば，$F(X) = (X^q + c_{q-1}X^{q-1} + \cdots + c_0)^p$（1.7 節命題 1）となり，$F(X)$ は既約でなくなる．ところで，K が $p \neq 0$ を標数にもつ有限体ならば，K から K への写像 $x \mapsto x^p$ は単射である（$x^p = y^p$ ならば $x^p - y^p = 0$ となり $(x-y)^p = 0$ となるから，$x - y = 0$ を得る）．K が有限であるから，これは全射となる．ゆえに，上で述べたことより $F(X)$ は既約でないことになり，矛盾する．　□

☞ 標数 $p \neq 0$ の体 K で，$x \mapsto x^p$ が全射（すなわち，K の任意の元は p 乗の形で書ける）が成り立つとき，K は**完全体** (perfect field) といわれる．有限体は完全体であることが上の補題の証明からいえたことになる．標数 0 の体は便宜上完全体と考えることにする．前述の補題は任意の完全体についても成り立つ（ここでの証明は一般の場合にも通用する）．$\mathbb{F}_p$ の 1 変数の有理関数体 $\mathbb{F}_p(T)$ は完全体ではない．なぜならば，変数 T は $\mathbb{F}_p(T)$ の元の p 乗では書けないからである．

定理 1. K を標数 0 の体または有限体，K' を K の n 次の有限拡大，C を K を含む代数的閉体とする．このとき，K' から C の中への n 個の異なる K-同型が存在する．

証明　K' が $K[x]$ $(x \in K')$ の形のときは，この定理は成り立つ．実際，x の K 上の最小多項式 $F(X)$ は次数 n である．$F(X)$ は C において n 個の根 $x_1, \ldots, x_n$ をもち，補題によりそれらはすべて異なる．任意の $i = 1, \ldots, n$ に対して K-同型 $\sigma_i : K' \to C$ で $\sigma_i(x) = x_i$ であるものがある．

$K \subset K[x] \subset K'$ を考え，$q = [K[x] : K]$ とおく．$q > 1$ と仮定してよい．$K[x]$ から C の中への異なる q 個の K-同型 $\sigma_1, \ldots, \sigma_q$ があることは示してある．$K[\sigma_i(x)]$ と $K[x]$ は同型であることより，$K[\sigma_i(x)]$ の拡大 K'_i と同型 $\tau_i : K' \to K'_i$ で σ_i の延長であるものを作ることができる．明らかに $K[\sigma_i(x)]$ は標数 0 または有限体である．$[K'_i : K[\sigma_i(x)]] = [K' : K[x]] = n/q < n$ であるから，帰納法の仮定より異なる n/q 個の K'_i から C の中への $K[\sigma_i(x)]$-同型 θ_{ij} がある．よって合成写像 $\theta_{ij} \cdot \tau_i$ は $q \cdot (n/q) = n$ 個の K' から C の中への K-同型を与える．これらはすべて異なる．なぜならば，$i \neq i'$ のときは $\theta_{ij} \cdot \tau_i$ と $\theta_{i'j'} \cdot \tau_{i'}$ は $K[x]$ 上で異なり，$i = i'$ で $j \neq j'$ のときは θ_{ij} と $\theta_{ij'}$ は K'_i 上で異なるからである．　□

☞ 定理 1 は K が完全体の場合に拡張できる．完全体の代数拡大（特に $K[\sigma_i(x)]$）は完全体である．証明の残りの部分は変更なしで通用する．

系（原始元の定理）．K を有限体または標数 0 の体とする．K' を K の n 次の有限拡大とする．このとき，元 $x \in K'$ で $K' = K[x]$ となるもの（**原始元** (primitive element) といわれる）がある．

証明　K を有限体とすると，K' は有限体でその乗法群 K'^* はある 1 つの元 x のべきで構成される（1.7 節定理 1(b)）．よって $K' = K[x]$ となる．

K を標数 0 の体，したがって無限体とする．定理 1 より，K' から K を含む代数的閉体 C の中への n 個の K-同型 σ_i がある．$i \neq j$ に対して，方程式 $\sigma_i(y) = \sigma_j(y)$ $(y \in K')$ は K' の部分集合 V_{ij} を定義する．これは明らかにベクトル空間 K' の K-部分空間で，$\sigma_i \neq \sigma_j$ ならば K' と異なる．K は無限体であるから，線型代数の話より，V_{ij} の和集合は K' 全体とは異なる．$x \in K' \backslash \bigcup V_{ij}$ をとると，$\sigma_i(x)$ $(i = 1, \ldots, n)$ はどの 2 つも異なる．よって x の K 上の最小多項式 $F(X)$ は少なくとも n 個の異なる根 $\sigma_1(x), \ldots, \sigma_n(x)$ を C でもつ．ゆえに $\deg(F(X)) \geq n$，すなわち，$[K[x] : K] \geq n$ となる．$K[x] \subset K'$ で $[K' : K] = n$ であるから，$K' = K[x]$ となる．□

2.5　2 次体の整数

一般論の展開を少しの間休止して，例をあげよう．

定義．有理数体 $\mathbb{Q}$ 上の 2 次の拡大体を **2 次体** (quadratic field) という．

K を 2 次体とするとき，任意の $x \in K \setminus \mathbb{Q}$ は $\mathbb{Q}$ 上次数 2 であり，従って K の原始元（すなわち，$K = \mathbb{Q}[x]$，$\{1, x\}$ は K の $\mathbb{Q}$ 上の基底）となる．$F(X) = X^2 + bX + c$ $(b, c \in \mathbb{Q})$ をそのような元 $x \in K$ の最小多項式とする．2 次方程式 $x^2 + bx + c = 0$ を解くと $2x = -b \pm \sqrt{b^2 - 4c}$ となる．よって $K = \mathbb{Q}(\sqrt{b^2 - 4c})$ ‡となる．さて，$b^2 - 4c$ は有理数 $u/v = uv/v^2$ $(u, v \in \mathbb{Z})$ である．よって $K = \mathbb{Q}(\sqrt{uv})$，$uv \in \mathbb{Z}$ と書ける．実際，d を平方因子をもたない $\mathbb{Z}$ の元（d は異なる素数の積の正または負の数である）により，$K = \mathbb{Q}(\sqrt{d})$ と書ける．ゆえに次のことが成り立つ．

命題 1. 任意の 2 次体は $\mathbb{Q}(\sqrt{d})$ の形である．ここで d は平方因子をもたない整数である．

$\sqrt{d}$ は既約多項式 $X^2 - d$ の根である．$\sqrt{d}$ は K において共役元をもち，

‡ $\sqrt{b^2 - 4c}$ は平方して $b^2 - 4c$ となる K の 2 つの元のうちの 1 つを意味する．

それは $-\sqrt{d}$ でなければならない．K の自己同型 σ で $\sqrt{d}$ を $-\sqrt{d}$ に写すものがある（2.4 節）．任意の K の元は $a+b\sqrt{d}$ $(a,b\in\mathbb{Q})$ の形である．従って

$$\sigma(a+b\sqrt{d})=a-b\sqrt{d}. \tag{1}$$

K の**整数** (integer) の環 A，すなわち，$x\in K$ で $\mathbb{Z}$ 上整であるものの集合，を考える（2.1 節命題 1 の系 2）．もし $x\in A$ ならば，$\sigma(x)$ は x と同じ整従属の方程式の根である．よって $\sigma(x)\in A$ となる．従って $x+\sigma(x)\in A$，$x\cdot\sigma(x)\in A$ である．$x=a+b\sqrt{d}$ $(a,b\in\mathbb{Q})$ のとき，(1) により

$$x+\sigma(x)=2a\in\mathbb{Q},\qquad x\cdot\sigma(x)=a^2-db^2\in\mathbb{Q}. \tag{2}$$

$\mathbb{Z}$ は単項イデアル環であることより，整閉（2.2 節例 2）であるから，

$$2a\in\mathbb{Z},\qquad a^2-db^2\in\mathbb{Z} \tag{3}$$

となる．

$x=a+b\sqrt{d}$ が $\mathbb{Z}$ 上整であるためには条件 (3) は必要条件である．x は $X^2-2aX+a^2-db^2=0$ の根であるから，十分条件でもある．(3) によって，$(2a)^2-d(2b)^2\in\mathbb{Z}$ となる．$2a\in\mathbb{Z}$ であるから $d(2b)^2\in\mathbb{Z}$ もまた成り立つ．他方，d は平方因子をもたないことより，もし $2b$ が整数でないと仮定すると，その分母は素因数 p を含まなければならない．この素因数は $(2b)^2$ の分母の中では p^2 の形で現れなければならない．d を掛けることは $(2b)^2$ を $\mathbb{Z}$ の中に写さない．ゆえに $2b\in\mathbb{Z}$ と結論できる．

すなわち，$a=u/2$，$b=v/2$　$(u,v\in\mathbb{Z})$ ととってよい．条件 (3) は

$$u^2-dv^2\in 4\mathbb{Z} \tag{4}$$

となる．

もし v が偶数ならば，(4) より u も偶数である．この場合，$a,b\in\mathbb{Z}$ となる．もし v が奇数ならば，$v^2\equiv 1 \pmod 4$ となる．u^2 が mod 4 でとれる可能性は 0 と 1（mod 4 での平方数はこれのみ）．d は平方因子を含まないから，これは 4 の倍数ではない．必然的に $u^2\equiv 1 \pmod 4$ となり，$d\equiv 1 \pmod 4$ となる．このことより次の定理が得られる．

定理 1． $K=\mathbb{Q}(\sqrt{d})$ を 2 次体で，$d\in\mathbb{Z}$ は平方因子を含まない（ゆえに

$d \not\equiv 0 \pmod 4$）とする．

(a) $d \equiv 2$ または $d \equiv 3 \pmod 4$ ならば，K の整数環は $a+b\sqrt{d}$ $(a, b \in \mathbb{Z})$ の形の元で構成される．

(b) $d \equiv 1 \pmod 4$ ならば，A は $\frac{1}{2}(u+v\sqrt{d})$ （$u, v \in \mathbb{Z}$ で同じ奇偶性をもつ，すなわち，$u \equiv v \pmod 2$）の形の元で構成される．　□

$d \equiv 2$ または $3 \pmod 4$ の場合は $\{1, \sqrt{d}\}$ が A の $\mathbb{Z}$-加群としての基底である．

$d \equiv 1 \pmod 4$ のときは，$\{1, \frac{1}{2}(1+\sqrt{d})\}$ が A の $\mathbb{Z}$-加群としての基底になる．実際，(b) より 1 と $\frac{1}{2}(1+\sqrt{d})$ は A の元である．逆に，$\frac{1}{2}(u+v\sqrt{d})$ $(u, v \in \mathbb{Z}$ で同じ奇偶性をもつ）が 1 と $\frac{1}{2}(1+\sqrt{d})$ の 1 次結合として表されることを示すには，$\frac{1}{2}(1+\sqrt{d})$ を減ずることにより u と v が偶数である場合に還元すればよい．この場合は，

$$\frac{1}{2}(u+v\sqrt{d}) = \left(\frac{u}{2} - \frac{v}{2}\right) \cdot 1 + v \cdot \frac{1}{2}(1+\sqrt{d})$$

である．

いくつかの用語を与えて終えることにする．$d > 0$ ならば $\mathbb{Q}(\sqrt{d})$ は**実 2 次体** (real quadratic field) とよばれる（$\mathbb{Q}$ 上 $\mathbb{Q}(\sqrt{d})$ と共役な $\mathbb{R}$ の部分体が存在する）．$d < 0$ のときは，$\mathbb{Q}(\sqrt{d})$ は**虚 2 次体** (imaginary quadratic field) といわれる．

2.6 ノルムとトレース

(a) 線型代数の復習

A を環，E を有限階数 (finite rank) の自由 (free) A-加群，u を E の自己準同型 (endomorphism) とする．線型代数においては，トレース (trace)，行列式 (determinant)，特性多項式 (characteristic polynomial) が定義される．E の基底 $\{e_i\}$ が選ばれていて，(a_{ij}) をこの基底に関しての u の行列 (matrix) とすると，トレース，行列式，特性多項式はそれぞれ，

$$\operatorname{Tr}(u)=\sum_{i=1}^{n}a_{ii},\ \det(u)=\det(a_{ij}),\ \det(X\cdot I_E-u)=\det(X\delta_{ij}-a_{ij}) \quad (1)$$

で与えられる．

注意．これらは基底のとり方によらない．

公式 (1) より

$$\begin{cases} \operatorname{Tr}(u+u')=\operatorname{Tr}(u)+\operatorname{Tr}(u'), \\ \det(uu')=\det(u)\det(u'), \\ \det(X\cdot I_E-u)=X^n-(\operatorname{Tr}(u))X^{n-1}+\cdots+(-1)^n\det(u). \end{cases} \quad (2)$$

(b) 拡大環についてのノルムとトレース

B を環，A を B の部分環で B は有限階数 n の自由 A-加群とする（たとえば，A が体で B は A の n 次の有限拡大体）．$x\in B$ に対して，x を掛けるという写像 m_x（すなわち，$y\mapsto xy$ ）は A-加群 B の自己準同型である．

定義 1. $x\in B$ の A と B に関する**トレース**（あるいは，**ノルム**，**特性多項式**）とは，x を掛ける自己準同型 m_x のトレース（あるいは，ノルム，特性多項式）のこととする．

$x\in B$ のトレース（あるいは，ノルム）を $\operatorname{Tr}_{B/A}(x)$（あるいは，$\mathrm{N}_{B/A}(x)$）と記す．混乱のおそれがないときは，単に $\operatorname{Tr}(x),\mathrm{N}(x)$ と表す．これらは A の元である．特性多項式は A に係数をもつ最高次の係数が 1 の多項式である．

$x,x'\in B$ と $a\in A$ に対して，$m_x+m_{x'}=m_{x+x'},m_x\cdot m_{x'}=m_{xx'},m_{ax}=am_x$ が成り立つ．さらに，B の A 上の任意の基底に関する m_a の行列は主対角成分がすべて a の対角行列 (diagonal matrix) である．(1) と (2) より

$$\begin{matrix} \operatorname{Tr}(x+x')=\operatorname{Tr}(x)+\operatorname{Tr}(x'), & \operatorname{Tr}(ax)=a\operatorname{Tr}(x), & \operatorname{Tr}(a)=n\cdot a, \\ \mathrm{N}(xx')=\mathrm{N}(x)\mathrm{N}(x'), & \mathrm{N}(a)=a^n, & \mathrm{N}(ax)=a^n\mathrm{N}(x) \end{matrix} \quad (3)$$

を得る．

命題 1. K を標数 0 または有限体，L を K の n 次の代数拡大，x を L の元，$x_1,\ldots,x_n$ を x の K 上の最小多項式の（K の適当な拡大体における）

根とする（2.3 節命題 3 を参照）．ただし，それらは $[L:K[x]]$ 個ずつ繰り返してとられている．このとき，

$$\mathrm{Tr}_{L/K}(x) = x_1 + \cdots + x_n,$$
$$\mathrm{N}_{L/K}(x) = x_1 \cdots x_n,$$

x の L と K に関する特性多項式は $(X - x_1)\cdots(X - x_n)$

である．

∞ 従って特性多項式は x の K 上の最小多項式の $[L:K[x]]$ 乗である．

証明　最初に x が L の K 上原始的 (primitive) な元の場合について扱うことにする（2.4 節定理 1 の系を参照）．$F(X)$ を x の K 上の最小多項式とする．このとき，L は $K[X]/(F(X))$ と K-同型（2.3 節 (5)）となり，$\{1, x, x^2, \ldots, x^{n-1}\}$ が L の K 上の基底となる．$F(X) = X^n + a_1X^{n-1} + \cdots + a_1X + a_0$ とおくと，この基底に関する自己準同型 m_x の行列は

$$M = \begin{bmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & 0 & & \vdots & \vdots \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{bmatrix}$$

となる．よって $X \cdot I_L - m_x$ の行列式は，次の行列の行列式となる．

$$X \cdot I_n - M = \begin{bmatrix} X & 0 & \cdots & 0 & a_0 \\ -1 & X & \cdots & 0 & a_1 \\ 0 & -1 & \cdots & 0 & a_2 \\ \vdots & 0 & & \vdots & \vdots \\ \vdots & \vdots & & \vdots & \vdots \\ \vdots & \vdots & \cdots & X & a_{n-2} \\ 0 & 0 & \cdots & -1 & X + a_{n-1} \end{bmatrix}.$$

この行列式を X の多項式として展開すると，X の特性多項式を得る．それは明らかに x の最小多項式 $F(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ と等しい．(2) より，$\mathrm{Tr}(x) = -a_{n-1}$，$\mathrm{N}(x) = (-1)^n a_0$ となる．x は原始的であるから，$F(X) = (X - x_1)\cdots(X - x_n)$ であり，係数を比較することより，$\mathrm{Tr}(x) = x_1 + \cdots + x_n$，$\mathrm{N}(x) = x_1 \cdots x_n$ であることがわかる．

さて，一般の場合を考えよう．$r = [L : K[x]]$ とおく．x の L と K に関する特性多項式 $P(X)$ が x の K 上の最小多項式の r 乗に等しいことを示せば十分である．$\{y_i\}_{i=1,\dots,q}$ を $K[x]$ の K 上の基底とし，$\{z_j\}_{j=1,\dots,r}$ を L の $K[x]$ 上の基底とする．このとき $\{y_i z_j\}$ は L の K 上の基底で，$n = qr$ である（2.3 節命題 1）．ここで，$M = (a_{ih})$ を $K[x]$ において x 倍を表す基底 $\{y_i\}$ に関する行列とする．従って $xy_i = \sum_h a_{ih} y_h$ である．よって

$$x(y_i z_j) = \left(\sum_h a_{ih} y_h \right) z_j = \sum_h a_{ih} (y_h z_j)$$

となる．L の K 上の基底 $\{y_i z_j\}$ を辞書的順序で並べることにより，この基底に関して L において x 倍することを表す行列 M_1 は

$$M_1 = \begin{bmatrix} M & 0 & \cdots & 0 \\ 0 & M & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & M \end{bmatrix}$$

の形になる．すなわち，M は M_1 の対角ブロックとして r 回現れる．よって行列 $X \cdot I_n - M_1$ は r 個ある対角ブロックのそれぞれが $X \cdot I_q - M$ の形をしているものから構成される．結局，$\det(X \cdot I_n - M_1) = (\det(X \cdot I_q - M))^r$ となる．この等式の左辺は $P(X)$ であり，$\det(X \cdot I_q - M)$ は x の K 上の最小多項式であることが，この証明の最初の部分よりわかっている． □

最後に，整元のトレースとノルムに関する結果を示しておこう．

命題 2. A を整域，K をその分数体，L を K 上有限次の拡大，x を L の元で A 上整であるものとする．x の特性多項式 $P(X)$ のすべての係数，特に $\mathrm{Tr}_{L/K}(x)$ と $\mathrm{N}_{L/K}(x)$ は A 上整である．

証明　命題 1 を使う．$P(X)=(X-x_1)\cdots(X-x_n)$ と書けて，$P(X)$ の係数は符号の差異を除いて，$x_1,\dots,x_n$ による積同士の和で表される．すべての x_i が A 上整であることを示せば十分である（2.1 節命題 1 の系 1）．ところで各 x_i は K 上 x と共役であり（2.4 節），K-同型 $\sigma_i : K[x]\to K[x_i]$ で $\sigma_i(x)=x_i$ となるものがある．x の A 上の整従属の方程式に σ_i を作用させることにより，x_i の A 上の整従属の方程式が得られる．□

系． さらに A が整閉であるとする．このとき，x の特性多項式のすべての係数，特に $\mathrm{Tr}_{L/K}(x)$ と $\mathrm{N}_{L/K}(x)$ は A の元である．

証明　定義より，これらの係数は K の元である．命題 2 よりそれらは A 上整である．□

☞ 2 次体の議論（2.5 節）における $x+\sigma(x)$, $x\cdot\sigma(x)$ がそれぞれ X のトレースとノルムであったことに注意する．2 次体の議論の中において，上の系の特殊な場合（2.5 節 (3)）は証明している．

2.7　判別式

定義 1． B を環，A は B の部分環で B が有限階数 n の自由 A-加群であるものとする．$(x_1,\dots,x_n)\in B^n$ に対して，次の式で定義される A の元は集合 $\{x_1,\dots,x_n\}$ の**判別式** (discriminant) とよばれる．

$$D(x_1,\dots,x_n)=\det(\mathrm{Tr}_{B/A}(x_ix_j)). \tag{1}$$

命題 1． $(y_1,\dots,y_n)\in B^n$ を $y_j=\sum_{j=1}^{n}a_{ij}x_j$ $(a_{ij}\in A)$ と書かれる他の組とすると

$$D(y_1,\dots,y_n)=(\det(a_{ij}))^2D(x_1,\dots,x_n) \tag{2}$$

が成り立つ．

証明

$$\mathrm{Tr}(y_py_q)=\mathrm{Tr}\left(\sum_{i,j}a_{pi}a_{qj}x_ix_j\right)=\sum_{i,j}a_{pi}a_{qj}\mathrm{Tr}(x_ix_j)$$

である．これは行列の等式

$$(\mathrm{Tr}(y_p y_q)) = (a_{pi})(\mathrm{Tr}(x_i x_j)) \cdot {}^t(a_{qj})$$

を与える（ここで ${}^tM$ は行列 M の転置行列 (transpose) のことである）．証明を完成するにはこれらの行列式をとれば十分である． □

命題 1 は，B の A 上の基底の判別式同士は互いに A において随伴的である，すなわち，1 つの基底を他の基底によって表すときの行列 (a_{ij}) は成分が A の元となる逆行列をもつことを示している．従って，$\det(a_{ij})$ と $\det(a_{ij})^{-1}$ は A における単元である．ゆえに，次のように定義をすることができる．

定義 2. 定義 1 の仮定の下で，B の A 上の任意の基底の判別式によって生成される A の単項イデアルを B の A 上の**判別式** (discriminant) とよぶことにする．それを $\mathfrak{D}_{B/A}$ と表す．

命題 2. $\mathfrak{D}_{B/A}$ が零因子でない元を含むとする．このとき，$\{x_1, \ldots, x_n\} \subset B$ が B の A 上の基底であるための必要十分条件は $D(x_1, \ldots, x_n)$ が $\mathfrak{D}_{B/A}$ を生成することである．

証明 必要性はすでに証明されている．$d = D(x_1, \ldots, x_n)$ が $\mathfrak{D}_{B/A}$ を生成するとする．$\{e_1, \ldots, e_n\}$ を B の A 上の基底とする．$d' = D(e_1, \ldots, e_n)$ とおき，$x_i = \sum_{j=1}^n a_{ij} e_j$ ($a_{ij} \in A$, $1 \leq i \leq n$) とする．このとき，$d = \det(a_{ij})^2 d'$ である．仮定により $Ad = \mathfrak{D}_{B/A} = Ad'$ であった．ゆえに $b \in A$ が存在して $d' = bd$ となる．これより $d(1 - b\det(a_{ij})^2) = 0$．ここで d は零因子でない．なぜならば，そうでないとすると $Ad = \mathfrak{D}_{B/A}$ のすべての元が零因子になってしまうからである．ゆえに $1 - b\det(a_{ij})^2 = 0$ となる．これは $\det(a_{ij})$ が可逆元であることを意味する．よって行列 (a_{ij}) も可逆である．従って $\{x_1, \ldots, x_n\}$ は B の A 上の基底である． □

命題 3. K を有限体または標数 0 の体，L を K の n 次の有限拡大，$\sigma_1, \ldots, \sigma_n$ を L から K を含む代数的閉体 C の中への異なる n 個の K-同型とする（2.4 節定理 1）．このとき，$\{x_1, \ldots, x_n\}$ が L の K 上の基底であれば，

$$D(x_1, \ldots, x_n) = \det(\sigma_i(x_j))^2 \neq 0 \tag{3}$$

である．

証明　最初の等式は簡単な計算で得られる，すなわち

$$\begin{aligned}
D(x_1,\ldots,x_n) &= \det(\mathrm{Tr}(x_ix_j)) \\
&= \det(\sum_k \sigma_k(x_ix_j)) \\
&= \det(\sum_k \sigma_k(x_i)\sigma_k(x_j)) \\
&= \det(\sigma_k(x_i))\cdot\det(\sigma_k(x_j)) \\
&= \det(\sigma_i(x_j))^2.
\end{aligned}$$

残っているのは $\det(\sigma_i(x_j)) \neq 0$ を示すことである．$\det(\sigma_i(x_j)) = 0$ と仮定して矛盾を導こう．このとき $u_1,\ldots,u_n \in C$（どれかは 0 でない）が存在して，すべての j について $\sum_{i=1}^n u_i\sigma_i(x_j) = 0$ となる．線型性により $\sum_{i=1}^n u_i\sigma_i(x) = 0$ がすべての $x \in L$ について成り立つことになる．これは次の補題に矛盾する．

補題 (Dedekind)．G を群，C を体，$\sigma_1,\ldots,\sigma_n$ は G から乗法群 C^* への異なる準同型とする．このとき，$\sigma_1,\ldots,\sigma_n$ は C 上 1 次独立である（すなわち，すべての $g \in G$ に対して $\sum u_i\sigma_i(g) = 0$ ならば，$u_i \in C$ はすべて 0 となる）．

証明　$\sigma_1,\ldots,\sigma_n$ が 1 次従属だと仮定して，0 でない u_i の個数 q が最小であるような自明でない関係 $\sum_i u_i\sigma_i = 0$ $(u_i \in C)$ について考える．番号のつけかえをやって，任意の $g \in G$ に対して

$$u_1\sigma_1(g) + \cdots + u_q\sigma_q(g) = 0 \tag{4}$$

としてよい．$\sigma_1,\ldots,\sigma_q$ はすべて 0 でないから，$q \geq 2$ である．g, h を G の任意の元とすると，

$$u_1\sigma_1(hg) + \cdots + u_q\sigma_q(hg) = u_1\sigma_1(h)\sigma_1(g) + \cdots + u_q\sigma_q(h)\sigma_q(g) = 0$$

となる．(4) に $\sigma_1(h)$ を掛けて辺々ひくと，

$$u_2(\sigma_1(h)-\sigma_2(h))\sigma_2(g)+\cdots+u_q(\sigma_1(h)-\sigma_q(h))\sigma_q(g)=0$$

を得る．この式は任意の $g \in G$ に対して成り立ち，q が最小に選んであったことより，$u_2(\sigma_1(h)-\sigma_2(h)) = 0$ が成り立つ．$u_2 \neq 0$ であったから $\sigma_1(h)=\sigma_2(h)$ が任意の $h \in G$ について成り立つ．これは σ_i がすべて異なっているという仮定に矛盾する． □

注意． 命題 3 の条件の下で，$D(x_1,\ldots,x_n) \neq 0$ であることは双 1 次形式 $(x,y) \mapsto \mathrm{Tr}_{L/K}(xy)$ が**非退化** (non-degenerated) である，すなわち，すべての $y \in L$ について $\mathrm{Tr}_{L/K}(xy) \neq 0$ ならば $x=0$ となることを意味する．従って，各 $x \in L$ に K-線型写像 $s_x : y \mapsto \mathrm{Tr}_{L/K}(xy)$ を対応させる K-線型写像は，L からその双対 K-ベクトル空間 $\mathrm{Hom}_K(L,K)$ への単射である．L と $\mathrm{Hom}_K(L,K)$ は K 上同じ有限次元 n なので，$x \mapsto s_x$ は全単射となる．ベクトル空間とその双対空間の「双対基底」の存在は，L の K 上の任意の基底 $\{x_1,\ldots,x_n\}$ に対して基底 $\{y_1,\ldots,y_n\}$ があって

$$\mathrm{Tr}_{L/K}(x_iy_j)=\delta_{ij} \quad (1 \leq i,j \leq n) \tag{5}$$

が成り立つことを示している．ここでの注意は後に役立つであろう．

定理 1． A を整閉環，K をその分数体，L を K の n 次の有限拡大，A' を A の L における整閉包とする．K は標数が 0 とする．このとき，A' は階数 n の自由 A-加群の A-部分加群である．

証明 $\{x_1,\ldots,x_n\}$ を L の K 上の基底とする．各 x_i は K 上代数的であり，自明でない方程式 $a_nx_i^n+a_{n-1}x_i^{n-1}+\cdots+a_0=0$（すべての j について $a_j \in A$）をもつ．ここで $a_n \neq 0$ としてよい．a_n^{n-1} を掛けることにより，a_nx_i は A 上整であることがわかる．$x_i'=a_nx_i$ とおく．すると $\{x_1',\ldots,x_n'\}$ は L の K 上の基底になり，それらは A' に含まれる．

この定理の前の注意によって，L の K 上の他の基底 $\{y_1,\ldots,y_n\}$ があって $\mathrm{Tr}(x_i'y_j)=\delta_{ij}$（(5) を参照）となる．$z \in A'$ をとる．$\{y_1,\ldots,y_n\}$ は L の K 上の基底であるから，$z=\sum_{j=1}^n b_jy_j$ $(b_j \in K)$ と書ける．任意の i について $x_i' \in A'$ なので $x_i'z \in A'$ となる．よって $\mathrm{Tr}(x_i'z) \in A$ である（2.6 節命題

2 の系）．従って，$\mathrm{Tr}(x'_i z) = \mathrm{Tr}(\sum_j b_j x'_i y_j) = \sum_j b_j \mathrm{Tr}(x'_i y_j) = \sum_j b_j \delta_{ij}$ $= b_i$ となる．このことより，任意の i について $b_i \in A$ がいえたことになり，これは A' が自由 A-加群 $\sum_{j=1}^n Ay_j$ の部分加群であることを示している．□

系． 定理 1 の仮定に加えて，A が単項イデアル環であるとする．このとき，A' は階数 n の自由 A-加群となる．

証明　加えられた仮定の下では，自由 A-加群の部分加群は自由 A-加群であり（1.5 節定理 1(b)），階数 $\leq n$ である．他方，定理 1 の証明の途中で，A' は L の K 上の基底を含むことを見た．従って階数は n である．□

☞ 定理 1 の前にある注意がよくわからない読者は，演習としてこの定理に対してより計算的な証明を考えてみるとよい．上で用いた記号の下で，$d = D(x'_1, \ldots, x'_n)$ とおいて，$z = \sum_i c_i x'_i$ $(c_i \in K)$ が A 上整であれば $dc_i \in A$ となることを示せ（$\mathrm{Tr}(zx'_j)$ を計算し，Cramer の公式を用いる）．

判別式の計算例

K を有限体または標数 0 の体，$L = K[x]$ を K の n 次の有限拡大，$F(X)$ を x の K 上の最小多項式とする．このとき

$$D(1, x, x^2, \ldots, x^{n-1}) = (-1)^{\frac{1}{2}n(n-1)} \mathrm{N}_{L/K}(F'(x)) \tag{6}$$

となる（ここで，$F'(X)$ は $F(X)$ の導関数を表す）．$x_1, \ldots, x_n$ を K のある拡大体の中での $F(X)$ の根とする．これらは x と共役である（2.3 節命題 3，および 2.4 節）．このとき，

$$\begin{aligned} D(1, x, x^2, \ldots, x^{n-1}) &= \det(\sigma_i(x^j))^2 && \text{（命題 3 による）} \\ &= \det(x_i^j)^2 \\ &= \left(\prod_{i<j} (x_i - x_j) \right)^2 && \text{（Vandermonde による）} \\ &= (-1)^{\frac{n(n-1)}{2}} \prod_i \left(\prod_{j \neq i} (x_i - x_j) \right) \end{aligned}$$

$$= (-1)^{\frac{n(n-1)}{2}} \prod_i F'(x_i)$$

$$= (-1)^{\frac{n(n-1)}{2}} \mathrm{N}_{L/K}(F'(x))$$

（ここで，$F'(x_i)$ はすべて $F'(x)$ と共役であることに注意する）を得る．

特に，$F(x)$ が 3 項式 $X^n + aX + b$ $(a, b \in K)$ の場合に (6) を適用する．$y = F'(x)$ とおくと，

$$y = nx^{n-1} + a = -(n-1)a - nbx^{-1}$$

（ここで $x^n + ax + b = 0$ より $nx^{n-1} = -na - nbx^{-1}$ となることに注意する）を得る．これより，$x = -nb(y + (n-1)a)^{-1}$ となる．y の K 上の最小多項式は $b^{-1}F(-nb(Y + (n-1)a)^{-1})$ の分子であり，計算の結果は

$$(Y + (n-1)a)^n - na(Y + (n-1)a)^{n-1} + (-1)^n b^{n-1}$$

となる．y のノルムはこの多項式の $(-1)^n$ 倍，すなわち，

$$n^n b^{n-1} + (-1)^{n-1}(n-1)^{n-1}a^n$$

である．従って，

$$D(1, x, x^2, \ldots, x^{n-1}) = (n^n b^{n-1} + (-1)^{n-1}(n-1)^{n-1}a^n)(-1)^{\frac{n(n-1)}{2}} \quad (7)$$

となる．$n = 2$（あるいは $n = 3$）のときは，よく知られた $a^2 - 4b$（あるいは $-27b^2 - 4a^3$）が再発見される．

2.8 数体の用語

$\mathbb{Q}$ の有限（従って代数的）拡大は**代数体** (algebraic field)（または**数体** (number field)）とよばれる．数体 K について，$[K : \mathbb{Q}]$ を K の**次数** (degree) という．次数 2（あるいは，次数 3）の数体は 2 次体 (quadratic field)（2.5 節を参照）（あるいは，3 次体 (cubic field)）といわれる．数体は常に標数 0 である．

数体 K の元で $\mathbb{Z}$ 上整であるものは K の**整数** (integer) とよばれる．それらは K の部分環 A を構成する（2.1 節命題 1 の系 2）．この環 A は階数

$[K:\mathbb{Q}]$ の自由 $\mathbb{Z}$-加群である（2.7 節定理 1 の系）．$\mathbb{Z}$-加群 A の基底の判別式は $\mathbb{Z}$ の単数倍を除いて決まり（2.7 節定義 2），その単数は $\mathbb{Z}$ において平方数である（2.7 節命題 1）．これは $+1$ のみが可能である，すなわち，$\mathbb{Z}$-加群 A の判別式は $\mathbb{Z}$ の元である．これを**絶対判別式** (absolute discriminant) または K の**判別式**という．

ことばを略して，A に関する概念を K の，といういい方をしばしばする．従って K のイデアル (ideal)（あるいは，単数 (unit)）というときは，A のイデアル（あるいは，単数）を意味している．

2.9　円分体

1 のべき根によって $\mathbb{Q}$ 上で生成された数体を**円分体** (cyclotomic field) という．素数 p に対して，（たとえば，$\mathbb{C}$ における）1 の p 乗根を z とする．円分体 $\mathbb{Q}[z]$ を調べてみよう．z は多項式 X^p-1 の根である．$z\neq 1$ であるから，それは多項式 $(X^p-1)/(X-1)=X^{p-1}+X^{p-2}+\cdots X+1$ の根でもある．この多項式を**円分多項式** (cyclotomic polynomial) という．この多項式が $\mathbb{Q}$ 上既約である（すなわち，体 $\mathbb{Q}[z]$ は $\mathbb{Q}$ 上次数 $p-1$ である）かどうかは，明らかなことではない．既約であることを証明するために，次の事実が必要となる．

Eisenstein の既約判定基準．A を単項イデアル環，p を A の素元 (prime element) とする．多項式

$$F(X)=X^n+a_{n-1}X^{n-1}+\cdots+a_1X+a_0\in A[X]$$

は，a_i $(0\leq i\leq n-1)$ は p で割り切れるが a_0 については p^2 では割り切れないものとする．このとき，$F(X)$ は A の分数体において既約である．

証明　$F=G\cdot H$，ここで G,H は $K[X]$ の元でともに最高次の係数が 1 である多項式，と書けたとする．F の根は A 上整である．G または H の任意の根は F の根であるので，A 上整でもある．G（あるいは，H）のどの係数も G（あるいは，H）の根による積の和で表される．それらもまた A 上整である（2.1 節命題 1 の系 1）．A は単項イデアル環であるから，整閉であ

る（2.2 節例 2）．ゆえに $G \in A[X]$ かつ $H \in A[X]$ である．

さて，$\overline{F}, \overline{G}, \overline{H}$ を F, G, H の $(A/Ap)[X]$ での像とすると，$\overline{F} = \overline{G} \cdot \overline{H}$ である．a_i $(0 \leq i \leq n-1)$ の仮定より，$\overline{F} = X^n$ である．A/Ap は整域であるから，分解 $X^n = \overline{G} \cdot \overline{H}$ は必然的に $X^n = X^q \cdot X^{n-q}$ の形になる（なぜならば，$\overline{G}, \overline{H}$ はともに最高次の係数が 1 であるから）．よって $\overline{G} = X^q, \overline{H} = X^{n-q}$ となる．もし G と H がともに定数でないならば p は G と H の両方の定数項を割り切る．ゆえに p^2 は F の定数項 a_0 を割り切る．これは仮定に矛盾する．よって，G または H のどちらかは定数でなければならないことになり，F は既約であることがいえた． □

例. 多項式 $X^3 - 2X + 6$ は $\mathbb{Q}$ 上既約である（$p = 2, A = \mathbb{Z}$ ととればよい）．

定理 1. 任意の素数 p に対して，円分多項式 $X^{p-1} + X^{p-2} + \cdots + X + 1$ は $\mathbb{Q}[X]$ において既約である．

証明 $X = Y + 1$ とおく．このとき，

$$\begin{aligned} X^{p-1} + X^{p-2} + \cdots + X + 1 &= \frac{X^p - 1}{X - 1} = \frac{(Y+1)^p - 1}{Y} \\ &= Y^{p-1} + \sum_{j=1}^{p-1} \binom{p}{j} Y^{p-j-1} \\ &= F_1(Y) \end{aligned}$$

とする．もし $F_1(Y)$ が既約であれば，もとの円分多項式もそうである．p は各二項係数 $\binom{p}{j}$ を割り切り，p^2 は定数項 $\binom{p}{1} = p$ を割り切らないから，$F_i(Y)$ は既約である（Eisenstein の既約判定基準）． □

定理 1 は $\mathbb{Q}[z]$ が次数 $p-1$ であることを示している．従って，$\{1, z, \ldots, z^{p-2}\}$ は $\mathbb{Q}[z]$ の $\mathbb{Q}$ 上の基底である．$\mathbb{Q}[z]$ の整数環を調べ，それが $\mathbb{Z}[z]$ であることを示すことにしよう．

このためには，トレースとノルム（$\mathrm{Tr}_{\mathbb{Q}[z]/\mathbb{Q}}(x)$，$\mathrm{N}_{\mathbb{Q}[z]/\mathbb{Q}}(x)$ の代わりに $\mathrm{Tr}(x)$，$\mathrm{N}(x)$ と表す）の計算をする必要がある．z の $\mathbb{Q}$ 上の共役元は z^j $(j = 1, \ldots, p-1)$（定理 1）であることに注意する．

円分多項式の既約性によりすぐわかることは

$$\mathrm{Tr}(z) = -1, \qquad \mathrm{Tr}(1) = p - 1. \tag{1}$$

従って $\mathrm{Tr}(z^j) = -1$ $(j = 1, \ldots, p-1)$．よって

$$\mathrm{Tr}(1-z) = \mathrm{Tr}(1-z^2) = \cdots = \mathrm{Tr}(1-z^{p-1}) = p \tag{2}$$

である．他方，定理 1 でなされた計算より $\mathrm{N}(z-1) = (-1)^{p-1}p$．これより $\mathrm{N}(1-z) = p$ となる．$1-z$ のノルムは $1-z$ の共役元のすべての積であったから，

$$p = (1-z)(1-z^2)\cdots(1-z^{p-1}) \tag{3}$$

となる．さて，A を $\mathbb{Q}[z]$ の整数環とする．明らかに A は z を含み，そのべきも含む．これから次の等式を示すことにする．

$$A(1-z) \cap \mathbb{Z} = p\mathbb{Z}. \tag{4}$$

$p \in A(1-z)$（公式 (3)）であることはわかっている．よって $A(1-z)\cap\mathbb{Z} \supset p\mathbb{Z}$ を得る．$p\mathbb{Z}$ は $\mathbb{Z}$ の極大イデアルであるから，もし $A(1-z)\cap\mathbb{Z} \neq p\mathbb{Z}$ ならば $A(1-z)\cap\mathbb{Z} = \mathbb{Z}$ となる，すなわち，$1-z$ は A の単元である．しかし，この場合，$1-z$ の共役元 $1-z^j$ もすべて単元でなければならず，(3) によって p は $A\cap\mathbb{Z}$ で単元でなければならなくなる．よって p^{-1} は $\mathbb{Z}$ に属することになるが，これは不合理である（2.2 節例 2）．

任意の $y \in A$ について，

$$\mathrm{Tr}(y(1-z)) \in p\mathbb{Z} \tag{5}$$

が成り立つことを示そう．$y(1-z)$ の各共役元 $y_j(1-z^j)$ は $1-z^j$ の（A における）倍元であり，（$1-z^j = (1-z)(1+z+\cdots+z^{j-1})$ であるから）$1-z^j$ 自身 $1-z$ の倍元である．トレースは共役元の和であるから，$\mathrm{Tr}(y(1-z)) \in A(1-z)$ である．よって (5) は (4) より直ちに出る．なぜならば，整数のトレースは $\mathbb{Z}$ に属する（2.6 節命題 2 の系）からである．

さて，これで $\mathbb{Q}[z]$ の整数環を決定する準備ができた．

定理 2. p を素数，z を（$\mathbb{C}$ における）1 の原始 p 乗根とする．このとき，

円分体 $\mathbb{Q}[z]$ の整数環 A は $\mathbb{Z}[z]$ であり，$\{1, z, \ldots, z^{p-2}\}$ は $\mathbb{Z}$-加群 A の基底である．

証明　$x = a_0 + a_1 z + \cdots + a_{p-2}z^{p-2}$ $(a_i \in \mathbb{Q})$ を A の元とする．このとき

$$x(1-z) = a_0(1-z) + a_1(z-z^2) + \cdots + a_{p-2}(z^{p-2} - z^{p-1}).$$

トレースをとって (1) と (2) を用いると，

$$\mathrm{Tr}(x(1-z)) = a_0 \mathrm{Tr}(1-z) = a_0 p$$

を得る．(5) より $pa_0 \in p\mathbb{Z}$ なので，$a_0 \in \mathbb{Z}$ となる．$z^{-1} = z^{p-1}$ であるから，$z^{-1} \in A$．従って

$$(x - a_0)z^{-1} = a_1 + a_2 z + \cdots a_{p-2}z^{p-3} \in A$$

となる．前と同様にして，$a_1 \in \mathbb{Z}$．順次同じ議論を重ねて，$a_i \in \mathbb{Z}$ を得る．

□

∞ **注意**．この節の結果は，t を 1 の p^r 乗根（p は素数）とするときの円分体 $\mathbb{Q}[t]$ の場合に対しても容易に拡張できる．そのような体は次数が $p^{r-1}(p-1)$ であり，その整数環は $\mathbb{Z}[t]$ となる．t の $\mathbb{Q}$ 上の最小多項式は

$$X^{p^{r-1}(p-1)} + X^{p^{r-1}(p-2)} + \cdots + X^{p^{r-1}} + 1 = \frac{X^{p^r} - 1}{X^{p^{r-1}} - 1}$$

である．

付　録

複素数体 $\mathbb{C}$ は代数的に閉じている

K を体として，次のことがらを考える．

(a) K 上の正次数の任意の多項式は次数 1 の多項式（線型多項式）の積である．

(b) 正次数の任意の多項式は K で根をもつ．

明らかに (a) ならば (b) が成り立つ．逆に，もし (b) が正しく，$P(X)$ を次

数 $d \geq 1$ の K 上の多項式で $a \in K$ が $P(X)$ の根であるとすれば，$P(X)$ は $X - a$ の倍元であり，$P(X)$ の次数 d についての帰納法で (a) が正しいことがいえる．同値な条件 (a) と (b) をみたす体 K は**代数的に閉じている** (algebraically closed) といわれる．

これから（本質的に）Lagrange による方法で，$\mathbb{C}(= \mathbb{R}[i], i^2 = -1)$ が代数的に閉じていることを示そう．次のことがらのみを用いる．

(1) 奇数次数をもつ $\mathbb{R}$ 上の多項式は $\mathbb{R}$ において根をもつ．これは Weierstrass の中間値の定理の特別な場合である．

(2) $\mathbb{C}$ 上の 2 次の多項式は $\mathbb{C}$ の中で根をもつ．$aX^2 + bX + c = 0$ の根についての初歩的な「公式」は，任意の $z = a + ib \in \mathbb{C}$ $(a, b \in \mathbb{R})$ は $\mathbb{C}$ において 2 乗根をもつという問題に帰着させられる．しかし，$(x + iy)^2 = a + ib$ $(x, y \in \mathbb{R})$ は $x^2 - y^2 = a, 2xy = b$ と同値であり，これより $a^2 + b^2 = (x^2 + y^2)^2$，そして $x^2 + y^2 = \sqrt{a^2 + b^2}$ を得る．明らかに，x^2 と y^2 を見つけることができ，よってこれらの式をみたす x, y が見つかる．

(3) 定数でない多項式 $P(X) \in K[X]$ が与えられたとき，K の拡大 K' で，$P(X)$ が $K'[X]$ において 1 次式の積に分解するようなものがある．この事実の簡単な証明が 2.3 節の命題 3 にあった（証明はこの章の他の結果とはほとんど独立したものである．$F(X)$ が既約のとき，$K[X]/(F(X))$ が体であることを示せば十分であり，あとは帰納法による）．

(4) 多項式の根と係数との関係．

(5) 対称多項式 (symmetric polynomial) $G(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$ は $X_1, \ldots, X_n$ の基本対称式 $\sum X_i$，$\sum X_i X_j$，$\ldots$，$X_1 \cdots X_n$ の多項式で表される．

定理． 複素数体 $\mathbb{C}$ は代数的に閉じている．

証明　性質 (b)，すなわち，定数でない多項式は $\mathbb{C}$ において根をもつこと，を

示す．$\overline{P}(X)$ を $P(X)$ の係数を複素共役にしたもので作られた多項式とする．$F(X) = P(X)\overline{P}(X) \in \mathbb{R}[x]$．なぜならば $\overline{F}(X) = F(x)$ だからである．このとき $F(X)$ が $\mathbb{C}$ で根をもつことは $P(X)$ が $\mathbb{C}$ で根をもつことと同値であることがわかるから，実数係数の多項式のみを考えればよいことがわかる．

さて，$F(X)(\in \mathbb{R}[X])$ の次数を $d = 2^n q$ と表す．ここで q は奇数である．2 の指数 n についての帰納法で議論を進める．$n = 0$ のときは d は奇数で $\mathbb{R}$ の中で根をもつ（(1) を参照）．$n \geq 1$ とする．$F(X)$ は最高次の係数が 1 としても一般性は失われない．(3) によって $\mathbb{C}$ の拡大 K' と $x_1, \ldots, x_d \in K'$ が存在して $F(X) = \prod_{i=1}^{d}(X - x_i)$ と書ける．

c を $\mathbb{R}$ の任意の元とし，$y_{ij} = x_i + x_j + cx_ix_j \in K'$ $(i \leq j)$ を考える．$\{y_{ij}\}$ $(1 \leq i \leq j \leq d)$ の個数は $\frac{1}{2}d(d+1) = 2^{n-1}q(d+1)$ である．ここで，$q(d+1)$ は奇数であることに注意する．多項式 $G(X) = \prod_{i \leq j}(X - y_{ij})$ は $x_1, \ldots, x_n$ についての実係数の対称多項式を係数としてもつ．(5) によりその係数は $x_1, \ldots, x_n$ の基本対称式の多項式であり，これらの多項式自身は実係数をもつ．従って，$G(X)$ の係数は実数である（(4) を参照）．$G(X)$ の次数は $2^{n-1}x$（x は奇数）であるから，帰納法の仮定により，それは根 $z_c \in \mathbb{C}$ をもつ．従って y_{ij} の中の 1 つ，たとえば，$y_{i(c),j(c)} = x_{i(c)} + x_{j(c)} + cx_{i(c)}x_{j(c)}$ は z_c に等しい．

さて，$\mathbb{R}$ は無限体で，(i, j) $(i \leq j)$ の組は有限であるから，2 つの異なる c と c' で $i(c) = i(c')$, $j(c) = j(c')$ となるものがある．これらをそれぞれ r, s とおく．すると $x_r + x_s + cx_rx_s = z_c \in \mathbb{C}$ でかつ $x_r + x_s + c'x_rx_s = z_{c'} \in \mathbb{C}$ である．1 次結合の部分を取り除いて，$x_r + x_s \in \mathbb{C}$ と $x_rx_s \in \mathbb{C}$ を得る．従って (4) により x_r と x_s は $\mathbb{C}$ を係数にもつ 2 次方程式の根である．これより $x_r, x_s \in \mathbb{C}$（(2) を参照）．従って $F(X)$ は $\mathbb{C}$ において根をもつことがいえたので，定理は証明された． □

練習問題

1. 2.7 節の定理 1 は，K を標数 0 であることの代わりに有限体と仮定しても成り立つ．なぜか？ K が有限体の場合には何らかの興味があるものであろうか？

2*. A を整閉環，K をその分数体，$P(X) \in A[X]$ を最高次の係数が 1 の多項式とする．$P(X)$ が $K[X]$ で既約ならば，$A[X]$ においても既約であることを示せ（ヒント：$P(X)$ の根を K の拡大体の中で考える）．

3*. すべての正の整数 n に対して，$\mathbb{F}_q$ 上の次数 n で最高次の係数が 1 の既約多項式の個数を $f(n)$ とする．このとき $\sum_{d|n} df(d) = q^n$ であることを示せ（ヒント：$\mathbb{F}_{q^n}$ の元を $\mathbb{F}_q$ 上の最小多項式によって分類する．$\mathbb{F}_{q^d} \subset \mathbb{F}_{q^n} \Leftrightarrow d|n$ に注意する）．このことより，値 $f(1), f(2), f(3), f(4)$ と素数 p についての $f(p)$ を求めよ．

4. 整閉でない整域の例を求めよ（2.5 節を参照）．

5*. R を環，A を R の部分環，x を R の単元とする．任意の $y \in A[x] \cap A[x^{-1}]$ は A 上整であることを示せ（ヒント：ある整数 n があって，A-加群 $M = A + Ax + \cdots + Ax^n$ が y を掛けることについて安定している，すなわち，$yM \subset M$ である，ことを示す．この点に立って 2.1 節の定理 1 の証明の後半を参照して証明に必要なアイディアを見いだす）．

第III章　Noether環とDedekind環

なぜ Dedekind 環について議論するのかということについては 3.4 節の例と定理 1 に続く議論を参照されたい．Noether 環は Dedekind 環よりもっと一般化されたものである．Noether 環を定義し，また Noether 環のもつ性質を自然な流れの中で使うために，その性質のいくつかを発展させよう．もちろん Noether 環が代数や代数幾何などの他の分野において基本的な重要性をもつからでもある．最後に，Noether 環に関してのある結論を Noether 加群の場合に一般化することは,「線型化」のもう 1 つの例であり，これは読者がすでに見てきた手法である．

3.1　Noether 環と加群

1.4 節で次のことが証明されている．

定理 1. A を環，M を A-加群とする．次の条件は同値である．

(a) M の空でない任意の部分加群の族は極大元をもつ．

(b) M の部分加群の任意の増大列は静止する．

(c) M の任意の部分加群は有限型である．

定義 1. A-加群 M は，定理 1 の同値条件をみたすとき **Noether 的** (Noetherian) であるとよばれる．環 A は，A-加群として Noether 加群のとき

Noether 環 (Noetherian ring) であるという．

（1.4 節定理 1 の系において）単項イデアル環は Noether 環であることを見た．

命題 1. A を環，E を A-加群，E' を E の部分加群とする．このとき，E が Noether 的であるためには E' と E/E' がともに Noether 的であることが必要十分条件である．

証明　最初に，必要条件であることを示す．E を Noether 的とする．E'（あるいは，E/E'）の部分加群の順序集合は E' に含まれる（あるいは，E' を含む）E の部分加群の順序集合と同型である．よって E' と E/E' は (a) または (b) より Noether 的である．

逆に，E' と E/E' が Noether 的であるとする．$\{F_n\}_{n\geq 0}$ を E の部分加群の増大列とする．E' は Noether 的であるから，ある整数 n_0 があって，任意の $n \geq n_0$ に対して $F_n \cap E' = F_{n+1} \cap E'$ となる．E/E' が Noether 的であるから，ある整数 n_1 があって，任意の $n \geq n_1$ に対して $(F_n + E')/E' = (F_{n+1} + E')/E'$ となる．従って，任意の $n \geq n_1$ に対して $F_n + E' = F_{n+1} + E'$ となる．$n \geq \sup\{n_0, n_1\}$ となる n をとる．$F_n = F_{n+1}$ であることを示そう．そのためには，$F_{n+1} \subset F_n$ を示せば十分である．これを見るために，$x \in F_{n+1}$ をとる．$F_{n+1} + E' = F_n + E'$ であるから，$y \in F_n$ と $z', z'' \in E'$ が存在して，$x + z' = y + z''$ となる．よって $x - y = z'' - z' \in F_{n+1} \cap E'$ である．$F_{n+1} \cap E' = F_n \cap E'$ であった．よって，$x - y$ と y は F_n に属するから $x \in F_n$ でもある．これで任意の $n \geq \sup\{n_0, n_1\}$ に対して $F_{n+1} = F_n$ がいえた．ゆえに (b) より E は Noether 的である． □

系 1. A を環，$E_1, \ldots, E_n$ を Noether A-加群とする．このとき，A-加群の直積 $\prod_{i=1}^{n} E_i$ は Noether 的である．

証明　$n = 2$ のとき，E_1 は $E_1 \times E_2$ の部分加群 $E_1 \times (0)$ と同一視でき，これに対応する剰余加群は E_2 と同型である．よって命題 1 より結論を得る．

一般の場合は n に関する帰納法で証明できる. □

系 2. A を Noether 環, E を有限型の A-加群とする. このとき, E は Noether 加群である（従って, その任意の部分加群は有限型である）.

証明 1.4 節により, E は A^n の剰余加群（n は E の生成元からなる有限集合の濃度）と同型である. 系 1 より A^n は Noether 的であり, このことと命題 1 を組み合わせると, E が Noether 的であることがいえる. □

3.2 整元についての応用

命題 1. A を整閉な Noether 環とする. K をその分数体, L を K の有限拡大, A' を A の L における整閉包とする. K の標数は 0 とする. このとき, A' は有限型の A-加群であり, Noether 環である.

証明 A' が階数 n の自由 A-加群の部分加群であることはわかっている（2.7 節定理 1）. よって A' は有限型の A-加群（3.1 節命題 1 の系 2）であり, 従って Noether 加群（同上）である. 他方, A' のイデアルは A' の A-部分加群の特殊なものである. それらは極大条件（3.1 節定理 1(a)）をみたし, 従って A' は Noether 環である. □

例. 数体の整数環は Noether 環である（$A = \mathbb{Z}$, $K = \mathbb{Q}$ ととればよい）.

3.3 イデアルについての準備

環 A のイデアル $\mathfrak{p}$ は $A/\mathfrak{p}$ が整域になるとき**素** (prime) イデアルとよばれる. 同じことであるが, $x \in A \setminus \mathfrak{p}, y \in A \setminus \mathfrak{p}$ ならば $xy \in A \setminus \mathfrak{p}$ である. すなわち, $A \setminus \mathfrak{p}$ は乗法に関して閉じているということである.

A のイデアル $\mathfrak{m}$ が**極大** (maximal)（すなわち, A と異なる A のイデアルの中で極大）であるためには $A/\mathfrak{m}$ がそれ自身と (0) 以外にイデアルをもたないこと, すなわち, $A/\mathfrak{m}$ が体であることが必要十分である. よって, すべての極大イデアルは素イデアルである. この逆は成り立たない. なぜなら

$\mathbb{Z}$ のイデアル (0) は素イデアルであるが極大イデアルではないからである．

補題 1. A を環，$\mathfrak{p}$ を A の素イデアル，A' を A の部分環とする．このとき，$\mathfrak{p} \cap A'$ は A' の素イデアルである．

証明　$\mathfrak{p} \cap A'$ は準同型の合成 $A' \to A \to A/\mathfrak{p}$ の核である．よって単射準同型 $A'/\mathfrak{p} \cap A' \to A/\mathfrak{p}$ が存在する．明らかに，整域の部分環は整域である．□

環 A の 2 つのイデアル $\mathfrak{a}$ と $\mathfrak{b}$ が与えられたとき，$\mathfrak{a}$ と $\mathfrak{b}$ の**積** (product) を単に積 ab $(a \in \mathfrak{a}, b \in \mathfrak{b})$ の集合とするのではなく，そのような積の**有限和** $\sum a_i b_i$ の集合として定義する．直ちにわかるように $\mathfrak{ab}$ は A のイデアルであり，次の包含関係

$$\mathfrak{ab} \subset \mathfrak{a} \cap \mathfrak{b} \tag{1}$$

が成り立つ．

∞ この両辺は必ずしも等しくはない．単項イデアル環のときは，左辺はイデアルの生成元の積に対応し，右辺は生成元の最小公倍元に対応している．

イデアルの積は結合的で可換である．A は，この単位元をもつ半群において，単位元にあたる．

∞ A-加群 E，E の部分加群 F，A のイデアル $\mathfrak{a}$ が与えられたとき，同様にして積 $\mathfrak{a}F$ が定義される．これは E の部分加群である．

補題 2. 環 A の素イデアル $\mathfrak{p}$ がイデアルの積 $\mathfrak{a}_1 \cdots \mathfrak{a}_n$ を含むならば，$\mathfrak{p}$ は少なくとも 1 つのイデアル $\mathfrak{a}_i$ を含む．

証明　すべての i について $\mathfrak{a}_i \not\subset \mathfrak{p}$ とすると，各 i に対して元 $a_i \in \mathfrak{a}_i \setminus \mathfrak{p}$ が存在する．従って，$\mathfrak{p}$ が素イデアルであるから $a_1 \cdots a_n \notin \mathfrak{p}$ となる．ところが $a_1 \cdots a_n \in \mathfrak{a}_1 \cdots \mathfrak{a}_n$ であるから，矛盾である．□

補題 3. Noether 環においては，任意のイデアルはある素イデアルの積を含む．Noether 整域においては，(0) でない任意のイデアルは (0) でないある素

イデアルの積を含む.

証明 Noether 環の理論においてかなり頻繁に現れるタイプの議論を用いることにしよう. 第2の主張を証明する (第1についての証明は類似のものとして考えられる. すなわち「(0) でない」ということばを3回取り除くだけでよい). (0) でない素イデアルの積を含まない, A の (0) でないイデアルの族 Φ は空でないと仮定し, 矛盾を探そう. A は Noether 環であるから, Φ は極大元 $\mathfrak{b}$ を含む (3.1 節定理 1(a)). イデアル $\mathfrak{b}$ は素イデアルではありえない. そうでないとすると $\mathfrak{b}$ は Φ に属さないからである. よって元 $x, y \in A \setminus \mathfrak{b}$ があって, $xy \in \mathfrak{b}$ となる. イデアル $\mathfrak{b} + Ax$ と $\mathfrak{b} + Ay$ はともに $\mathfrak{b}$ を真の部分集合として含む. 従って, $\mathfrak{b}$ が極大であることより, これらは Φ に属さない. これより, これらはともに (0) でない素イデアルの積をそれぞれ含んでいる, すなわち

$$\mathfrak{b} + Ax \supset \mathfrak{p}_1 \cdots \mathfrak{p}_n, \quad \mathfrak{b} + Ay \supset \mathfrak{q}_1 \cdots \mathfrak{q}_r.$$

$xy \in \mathfrak{b}$ であるから

$$(\mathfrak{b} + Ax)(\mathfrak{b} + Ay) \subset \mathfrak{b}$$

となり, これより $\mathfrak{p}_1 \cdots \mathfrak{p}_n \mathfrak{q}_1 \cdots \mathfrak{q}_r \subset \mathfrak{b}$ を得る. □

さて, A を整域, K をその分数体とする. K の A-部分加群 I で, ある $d \in A \setminus (0)$ があって $dI \subset A$ となるものを A の (または, K の A に関しての) **分数イデアル** (fractional ideal) とよぶ. これは, I のすべての元は「共通分母」$d \in A$ をもつことを意味する. A の通常のイデアルは分数イデアルである ($d = 1$ がとれる). これらを**整イデアル** (integral ideal) といって, 分数イデアルと区別することもある. K に含まれる有限型の A-加群 I は分数イデアルである. これは, もし $\{x_1, \ldots, x_n\}$ が I の生成元からなる有限集合とすると, 各 x_i は共通の分母 d (たとえば, $x_i = a_i d_i^{-1}$, $a_i, d_i \in A$ のとき d_i の積) をもち, d は I の共通分母である. 逆に, A が Noether 環のとき, すべての分数イデアル I は有限型の A-加群である. すなわち, $I \subset d^{-1}A$ で $d^{-1}A$ は A-加群として A と同型であるから Noether 的である.

2つの分数イデアル I, I' の**積** (product) II' を有限和 $\sum x_i y_i$ ($x_i \in$

I, $y_i \in I'$) の集合として定義する．もし I と I' が分数イデアルで，共通分母をそれぞれ d, d' とするならば，集合

$$I \cap I', \quad I + I', \quad II'$$

はすべて分数イデアルである．これらは明らかに K の A-部分加群であり，共通分母としてそれぞれ d（または d'），dd' と dd' をもつ．(0) でない A の分数イデアル全体は積について単位元をもつ可換な半群をなす．

3.4　Dedekind 環

定義 1. 整域 A は，整閉な Noether 環であって，(0) でないすべての素イデアルが極大であるとき，**Dedekind 環** (Dedekind domain) とよばれる．

環 $\mathbb{Z}$，さらには任意の単項イデアル環は Dedekind 環である．次の定理は，数体における整数環が Dedekind 環であることを示している．

定理 1. A を Dedekind 環，K をその分数体，L を K の有限拡大，A' を L における A の整閉包とする．K の標数は 0 であるとする．このとき，A' は Dedekind 環であり，有限型の A-加群である．

証明　作り方より A' は整閉である．3.2 節の命題により，A' は Noether 環で，有限型の A-加群である．あとは，すべての A' の素イデアル $\mathfrak{p}'(\neq (0))$ が極大であることを示せばよい．このために，元 $x \in \mathfrak{p}' \setminus (0)$ を選び，x の A 上の整従属方程式で次数が最小のもの

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0 \quad (a_i \in A) \tag{1}$$

を考える．このとき $a_0 \neq 0$ である．なぜならば，そうでないと x をくくり出して割ることにより，より小さな次数の方程式が得られるからである．(1) により $a_0 \in A'x \cap A \subset \mathfrak{p}' \cap A$ である．よって，$\mathfrak{p}' \cap A \neq (0)$ である．$\mathfrak{p}' \cap A$ は A の素イデアル（3.3 節補題 1）であることより，$\mathfrak{p}' \cap A$ は A の極大イデアルであり，$A/\mathfrak{p}' \cap A$ は体である．$A/\mathfrak{p}' \cap A$ は $A'/\mathfrak{p}'$ の部分環と同一視してよく，そのとき $A'/\mathfrak{p}'$ は $A/\mathfrak{p}' \cap A$ 上整である（A' が A 上整であるか

ら）．よって $A'/\mathfrak{p}'$ は体である（2.1 節命題 3）．ゆえに $\mathfrak{p}'$ は極大である．□

数体の整数環は Dedekind 環であるが，必ずしも単項イデアル環であるとは限らない．このことより，Dedekind 環に興味が寄せられるのである．

例．$\mathbb{Q}[\sqrt{-5}]$ における整数環 $A = \mathbb{Z}[\sqrt{-5}]$ を考えてみよう（2.5 節定理 1）．まず

$$(1+\sqrt{-5})(1-\sqrt{-5}) = 2\cdot 3 \tag{2}$$

を確認しておこう．これら 4 つの因子のノルムはそれぞれ 6, 6, 4, 9 である．$1+\sqrt{-5}$ は A において自明でない因子をもてないことに注意する．なぜなら，そのような因子があったとしたら 6 の自明でない因子でなければならないが，方程式

$$a^2+5b^2=2 \quad と \quad a^2+5b^2=3$$

は $\mathbb{Z}$ において解をもたないので不可能である．もし A が単項イデアル環であるとすれば，素元 $1+\sqrt{-5}$ は (2) により積 $2\cdot 3$ を割るから，2 または 3 を割らなければならない．ところが，ノルムをとることにより，6 が 4 または 9 を割り切ることになり，これはありえない．

歴史的には，数論家 Kummer (1810–1893) はある種の数体の整数環は単項イデアル環でないことを知っていた（実際，ある種の円分体がそうである．Kummer はこのことを Fermat の方程式についての仕事との関わり合いの中で知ったのであった．1.2 節を参照のこと）．都合良く，せめて部分的にでもこの不都合を回避するために，彼と Dedekind (1831–1916) はイデアルの概念を導入したのであった．Dedekind は現在では彼の名前をもっている環について当時研究していた．単項イデアル環の最も重要な性質は素元に一意的に分解できることである．この性質のエレガントな一般化を Dedekind 環の中に見ることができる．Dedekind 環においては，イデアルは素イデアルの積に一意的に分解する．この一意分解について，興味深い多くの結果がある．ここでそれらを詳細に記述し，そして証明するつもりである．

定理 2. A を体でない Dedekind 環，K を A の商体とする．A の分数イデアル全体のなす単位元をもつ半群において，A のすべての極大イデアルは可逆である．

証明　$\mathfrak{m}$ を A の極大イデアルとする．このとき A は体でないから $\mathfrak{m} \neq (0)$ である．

$$\mathfrak{m}' = \{x \in K \mid x\mathfrak{m} \subset A\} \tag{3}$$

とおく．明らかに，$\mathfrak{m}$ は K の A-部分加群であり，$\mathfrak{m}$ の 0 でない任意の元は $\mathfrak{m}'$ の元に対しての共通分母となる．従って $\mathfrak{m}'$ は A の分数イデアルであり，$\mathfrak{m}\mathfrak{m}' = A$ を示せば十分である．(3) より $\mathfrak{m}\mathfrak{m}' \subset A$ を得る．他方，$A \subset \mathfrak{m}'$（$\mathfrak{m}$ が A のイデアルであるから）．よって $\mathfrak{m} = A\mathfrak{m} \subset \mathfrak{m}'\mathfrak{m}$．$\mathfrak{m}$ は極大で $\mathfrak{m} \subset \mathfrak{m}'\mathfrak{m} \subset A$ であることより，$\mathfrak{m}'\mathfrak{m} = A$ または $\mathfrak{m}'\mathfrak{m} = \mathfrak{m}$ となる．あとは $\mathfrak{m}'\mathfrak{m} = \mathfrak{m}$ がありえないことを示すことが残っている．

$\mathfrak{m}'\mathfrak{m} = \mathfrak{m}$ かつ $x \in \mathfrak{m}'$ とすれば，$x\mathfrak{m} \subset \mathfrak{m}$，$x^2\mathfrak{m} \subset x\mathfrak{m} \subset \mathfrak{m}$ となり，帰納法により任意の $n \in \mathbb{N}$ について $x^n\mathfrak{m} \subset \mathfrak{m}$ を得る．よって $\mathfrak{m}$ の 0 でない任意の元 $d \in \mathfrak{m}$ はすべての x のべき x^n $(n \in \mathbb{N})$ の共通分母である．これより $A[x]$ は A の分数イデアルである．A は Noether 環であるから，$A[x]$ は有限型の A-加群である（3.3 節最後のあたり）．よって x は A 上整である（2.1 節定理 1）．ところで，A は整閉である．よって $x \in A$ となり，結局 $\mathfrak{m}'\mathfrak{m} = \mathfrak{m}$ であることは $\mathfrak{m}' = A$ を示している．あとは，$\mathfrak{m}' = A$ が不可能であることを示せばよい．

このために，0 でない元 $a \in \mathfrak{m}$ をとる．イデアル Aa は 0 でない素イデアルの積 $\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_n$ を含む（3.3 節補題 3）．ここで n は最小のものであるとしてよい．$\mathfrak{m} \supset Aa \supset \mathfrak{p}_1\cdots\mathfrak{p}_n$ であり，これよりある i について $\mathfrak{m} \supset \mathfrak{p}_i$（3.3 節補題 2）である．$i = 1$ とする．$\mathfrak{p}_1$ は仮定より極大であるから，$\mathfrak{m} = \mathfrak{p}_1$ となる．$\mathfrak{b} = \mathfrak{p}_2\cdots\mathfrak{p}_n$ とおくと，このとき，$Aa \supset \mathfrak{m}\mathfrak{b}$ で $Aa \not\supset \mathfrak{b}$ である（n は最小にとってあるから）．よって元 $b \in \mathfrak{b}$ が存在して $b \notin Aa$ となる．$\mathfrak{m}\mathfrak{b} \subset Aa$ であることより，$\mathfrak{m}b \subset Aa$ となる．よって $\mathfrak{m}ba^{-1} \subset A$ である．$\mathfrak{m}'$ の定義 (3) より，これは $ba^{-1} \in \mathfrak{m}'$ を意味する．しかし $b \notin Aa$ であるから，$ba^{-1} \notin A$．よって $\mathfrak{m}' \neq A$ となる．　□

定理 3.　A を Dedekind 環，P を A の (0) でない素イデアル全体からなる集合とする．このとき，

(a)　任意の (0) でない A の分数イデアル $\mathfrak{b}$ は

$$\mathfrak{b} = \prod_{\mathfrak{p} \in P} \mathfrak{p}^{n_{\mathfrak{p}}(\mathfrak{b})} \tag{4}$$

と一意的に表される．ここで任意の $p \in P$ について $n_{\mathfrak{p}}(\mathfrak{b}) \in \mathbb{Z}$ で，ほとんどすべての（すなわち，有限個を除いた）$\mathfrak{p} \in P$ について $n_{\mathfrak{p}}(\mathfrak{b}) = 0$ である．

(b) A の (0) でない分数イデアル全体のなす単位元をもつ半群は群をなす．

証明 最初に (a) の前半，すなわち，任意の分数イデアル $\mathfrak{b}$ は素イデアルのべき（≥ 0 または ≤ 0）の積であることを示そう．$d\mathfrak{b} \subset A$ となるような，すなわち $d\mathfrak{b}$ が A の整イデアルとなる $d \in A \setminus (0)$ が存在し，$\mathfrak{b} = (d\mathfrak{b}) \cdot (Ad)^{-1}$ である．よって一般性を失うことなく，(a) を整イデアルについて証明すればよい．3.3 節の補題 3 におけるのと同様に，A の (0) でないイデアルで素イデアルの積とならないものの族 Φ を考えよう．Φ が空でないと仮定し，$\mathfrak{a}$ を Φ の極大元とする（A が Noether 環であることに注意）．このとき，A は素イデアルの空な族の積であるから，$\mathfrak{a} \neq A$ である．よって $\mathfrak{a}$ はある極大イデアル $\mathfrak{p}$ に含まれる．従って $\mathfrak{p}$ は $\mathfrak{a}$ を含む A の自明でないイデアルの族の中で極大な元である．$\mathfrak{p}'$ を $\mathfrak{p}$ の逆（分数）イデアルとする．$\mathfrak{a} \subset \mathfrak{p}$ であることより $\mathfrak{a}\mathfrak{p}' \subset \mathfrak{p}\mathfrak{p}' = A$ となる．さらに $\mathfrak{p}' \supset A$ より $\mathfrak{a}\mathfrak{p}' \supset \mathfrak{a}$ となる．実際，$\mathfrak{a}\mathfrak{p}' \neq \mathfrak{a}$ である（もし $\mathfrak{a}\mathfrak{p}' = \mathfrak{a}$ で $x \in \mathfrak{p}'$ とすれば，$x\mathfrak{a} \subset \mathfrak{a}$ で，すべての n に対して $x^n\mathfrak{a} \subset \mathfrak{a}$ となり，x は A 上整かつ $x \in A$ となってしまう（定理 2 におけるように）．しかし，これは不可能である．なぜならば $\mathfrak{p}' \neq A$（そうでないと $\mathfrak{p}' = A$ で，$\mathfrak{p}\mathfrak{p}' = \mathfrak{p}$ となる）からである）．イデアル $\mathfrak{a}$ が Φ において極大であることより，$\mathfrak{a}\mathfrak{p}' \notin \Phi$ となり，$\mathfrak{a}\mathfrak{p}' = \mathfrak{p}_1 \cdots \mathfrak{p}_n$ のように素イデアルの積と書ける．$\mathfrak{p}$ を掛けることにより，$\mathfrak{a} = \mathfrak{p}\mathfrak{p}_1 \cdots \mathfrak{p}_n$ を得る．よって任意の A の整イデアルは素イデアルの積に表される．

次に (a) の一意性を考える．

$$\prod_{\mathfrak{p} \in P} \mathfrak{p}^{n(\mathfrak{p})} = \prod_{\mathfrak{p} \in P} \mathfrak{p}^{m(\mathfrak{p})},$$

すなわち，

$$\prod_{\mathfrak{p} \in P} \mathfrak{p}^{n(\mathfrak{p}) - m(\mathfrak{p})} = A$$

と仮定する．もし $n(\mathfrak{p})-m(\mathfrak{p})\neq 0$ がある素イデアル $\mathfrak{p}\in P$ で起きたとすると，正と負の指数を分離して，

$$\mathfrak{p}_1^{\alpha_1}\cdots\mathfrak{p}_r^{\alpha_r}=\mathfrak{q}_1^{\beta_1}\cdots\mathfrak{q}_s^{\beta_s} \tag{5}$$

と表すことができる．ここで，すべての i,j について $\mathfrak{p}_i,\mathfrak{q}_j\in P$, $\alpha_i>0,\beta_j>0$, $\mathfrak{p}_i\neq\mathfrak{q}_j$ である．これより $\mathfrak{p}_1$ は $\mathfrak{q}_1^{\beta_1}\cdots\mathfrak{q}_s^{\beta_s}$ を含む．よってある j について $\mathfrak{p}_1\supset\mathfrak{q}_j$（3.3 節補題 2），たとえば $j=1$ として $\mathfrak{p}_1\supset\mathfrak{q}_1$．ところで，$\mathfrak{p}_1$ と $\mathfrak{q}_1$ はともに極大であるから $\mathfrak{p}_1=\mathfrak{q}_1$ となる．これは矛盾である．

最後に (4) は $\prod_{\mathfrak{p}\in P}\mathfrak{p}^{-n_\mathfrak{p}(\mathfrak{b})}$ が $\mathfrak{b}$ の逆イデアルであることを示しているから，(b) が得られる．　□

注意．Dedekind 環 A の (0) でない分数イデアル全体のなす単位元をもつ半群 $I(A)$ は群になることをちょうど示した．単項分数イデアル（すなわち，$x\in K^*$ がとれて，Ax の形のもの）全体は $I(A)$ の部分群 $F(A)$ をなす（$(Ax)(Ay)^{-1}=Axy^{-1}$ に注意する）．剰余群 $C(A)=I(A)/F(A)$ を A の**イデアル類群** (ideal class group) という．A が単項イデアル環であるためには $C(A)$ が唯 1 つの元からなることが必要十分条件である．

この節をいくつかの公式を与えることで完結することにしよう．$n_\mathfrak{p}(\mathfrak{b})$ は $\mathfrak{b}$ を素イデアルの積に分解（(4) を参照）したときの $\mathfrak{p}$ の指数を表す．

$$n_\mathfrak{p}(\mathfrak{a}\mathfrak{b})=n_\mathfrak{p}(\mathfrak{a})+n_\mathfrak{p}(\mathfrak{b}) \tag{6}$$

（証明は明白）．

$$\mathfrak{b}\subset A\Leftrightarrow n_\mathfrak{p}(\mathfrak{b})\geq 0 \quad \text{（任意の } \mathfrak{p}\in P \text{ に対して）} \tag{7}$$

（$\Rightarrow$ は定理 3 の証明の途中で見た．$\Leftarrow$ は明らか）．

$$\mathfrak{a}\subset\mathfrak{b}\Leftrightarrow n_\mathfrak{p}(\mathfrak{a})\geq n_\mathfrak{p}(\mathfrak{b}) \quad \text{（任意の } \mathfrak{p}\in P \text{ に対して）} \tag{8}$$

（$\mathfrak{a}\subset\mathfrak{b}$ は $\mathfrak{a}\mathfrak{b}^{-1}\subset A$ と同じである．(6), (7) を適用すればよい）．

$$n_\mathfrak{p}(\mathfrak{a}+\mathfrak{b})=\inf(n_\mathfrak{p}(\mathfrak{a}),n_\mathfrak{p}(\mathfrak{b})) \tag{9}$$

（$\mathfrak{a}+\mathfrak{b}$ は $\mathfrak{a}$ と $\mathfrak{b}$ のイデアルについての包含関係での最小上界である．(8) を

用いて証明は完了する）．

$$n_{\mathfrak{p}}(\mathfrak{a} \cap \mathfrak{b}) = \sup(n_{\mathfrak{p}}(\mathfrak{a}), n_{\mathfrak{p}}(\mathfrak{b})) \tag{10}$$

（最大下界についての類似の議論で，(8) を再度用いる）．

3.5　イデアルのノルム

この節では，K は数体，n はその次数，A は K の整数環とする．$\mathrm{N}_{K/\mathbb{Q}}(x)$ を $\mathrm{N}(x)$ と表すことにする．

命題 1. x を A の 0 でない元とすれば，$|\mathrm{N}(x)| = \mathrm{card}(A/Ax)$ である．

> ∞ $x \in A$ であるから $\mathrm{N}(x) \in \mathbb{Z}$（2.6 節命題 2 の系）である．よって上の式は意味をもつ．

証明 A は階数 n の自由 $\mathbb{Z}$-加群であり（2.8 節），Ax は A の $\mathbb{Z}$-部分加群である．x を掛けることにより A から Ax の上への同型になるから，Ax もまた階数 n である．1.5 節の定理 1 より，$\mathbb{Z}$-加群 A の基底 $\{e_1, \ldots, e_n\}$ で，$c_i \in \mathbb{N}$ を選んで $\{c_1e_1, \ldots, c_ne_n\}$ が Ax の基底になるようなものがある．さらに，Abel 群 A/Ax は有限 Abel 群 $\prod_{i=1}^{n} \mathbb{Z}/c_i\mathbb{Z}$ に同型であり，その位数は $c_1 \cdots c_n$ に等しい．A から Ax の上への $\mathbb{Z}$-線型写像 u を $u(e_i) = c_ie_i$ $(i = 1, \ldots, n)$ とすると，$\det(u) = c_1 \cdots c_n$ である．

一方，$\{xe_1, \ldots, xe_n\}$ も Ax の基底である．よって $\mathbb{Z}$-加群 Ax の自己同型 v で $v(c_ie_i) = xe_i$ となるものがある．このとき $\det(v)$ は $\mathbb{Z}$ の中で可逆であり，$\det(v) = \pm 1$ となる．ところで，$v \cdot u$ は x を掛ける写像であり，その行列式は定義より $\mathrm{N}(x)$ である（2.6 節定義 1）．$\det(v \cdot u) = \det(v) \cdot \det(u)$ であることより，$\mathrm{N}(x) = \pm c_1 \cdots c_n = \pm \mathrm{card}(A/Ax)$ という結論を得る．□

定義 1. A の (0) でない整イデアル $\mathfrak{a}$ に対して，$\mathrm{card}(A/\mathfrak{a})$ を $\mathfrak{a}$ のノルム (norm) といい，$\mathrm{N}(\mathfrak{a})$ と表す．

$\mathrm{N}(\mathfrak{a})$ は有限である．実際，a を $\mathfrak{a}$ の 0 でない元とすると $Aa \subset \mathfrak{a}$ で，

$A/\mathfrak{a}$ は A/Aa の剰余環と同一視できる．よって $\mathrm{card}(A/\mathfrak{a}) \leq \mathrm{card}(A/Aa)$．$\mathrm{card}(A/\mathfrak{a})$ は命題 1 より有限である．一方，単項イデアル Ab に対して $\mathrm{N}(Ab) = |\mathrm{N}(b)|$ であることは見た．

命題 2. $\mathfrak{a}$ と $\mathfrak{b}$ をともに A の (0) でない整イデアルとすれば，$\mathrm{N}(\mathfrak{a}\mathfrak{b}) = \mathrm{N}(\mathfrak{a})\mathrm{N}(\mathfrak{b})$ である．

証明 イデアル $\mathfrak{b}$ は極大イデアルの積に分解される (3.4 節定理 3) から，極大イデアル $\mathfrak{m}$ に対して $\mathrm{N}(\mathfrak{a}\mathfrak{m}) = \mathrm{N}(\mathfrak{a})\mathrm{N}(\mathfrak{m})$ を示せば十分である．$\mathfrak{a}\mathfrak{m} \subset \mathfrak{a}$ であるから，$\mathrm{card}(A/\mathfrak{a}\mathfrak{m}) = \mathrm{card}(A/\mathfrak{a})\cdot\mathrm{card}(\mathfrak{a}/\mathfrak{a}\mathfrak{m})$ である．よって $\mathrm{card}(\mathfrak{a}/\mathfrak{a}\mathfrak{m}) = \mathrm{card}(A/\mathfrak{m})$ を示せばよい．ところで，$\mathfrak{a}/\mathfrak{a}\mathfrak{m}$ は $\mathfrak{m}$ によって消えてしまう A-加群であるから，これは $A/\mathfrak{m}$ 上のベクトル空間と考えることができる．その部分空間は A-部分加群であり，イデアル $\mathfrak{q}$ で $\mathfrak{a}\mathfrak{m} \subset \mathfrak{q} \subset \mathfrak{a}$ となるものをとって $\mathfrak{q}/\mathfrak{q}\mathfrak{m}$ の形に書ける．3.4 節の公式 (8) により，$\mathfrak{a}\mathfrak{m}$ と $\mathfrak{a}$ の間にはイデアルが存在しない．従ってベクトル空間 $\mathfrak{a}/\mathfrak{a}\mathfrak{m}$ は $A/\mathfrak{m}$ 上次元 1 である．これより $\mathrm{card}(\mathfrak{a}/\mathfrak{a}\mathfrak{m}) = \mathrm{card}(A/\mathfrak{m})$ を得る．　□

練習問題

1. なぜ体は Dedekind 環であるか？

2. 3.4 節の定理 2 に述べた主張について，A が体でないという仮定が不必要であるようにするためには，主張をどう変えればよいか？

3*. Noether 環 A においては，A 自身と異なる任意のイデアルは極大イデアルに含まれることは明らかである．このことは A が Noether 環でないときも正しいことを示せ（ヒント：Zorn の補題を用いる）．

4. 整域 A で，ある A の素イデアル $\mathfrak{p} \neq (0)$ と部分環 A' に対して $A' \cap \mathfrak{p} = (0)$ となるものの例をあげよ．

5. K を体とする．2 変数の多項式環 $K[X, Y]$ は Dedekind 環か？

6*. K を体，A を多項式環 $K[X]$ の部分環 $K[X^2, X^3]$ とする．
(a) 包含関係 $K[X^2] \subset A \subset K[X]$ を用いて，A は Noether 環で，(0) でない任意のイデアルは極大イデアルであることを示せ．
(b) A は Dedekind 環でないことを示せ（ヒント：元 X を考えよ）．

第IV章　イデアル類と単数定理

この章は 2 つの重要な有限性定理にあてられる．これらの定理の証明には多少の解析学（$\mathbb{R}^n$ におけるトポロジーと積分を借用）が必要とされる．まず，この道具の展開から始めることにしよう．

4.1　$\mathbb{R}^n$ の離散部分群についての準備

$\mathbb{R}^n$ の部分群 H が **離散的** (discrete) であるとは，$\mathbb{R}^n$ の任意のコンパクト (compact) 部分集合 K に対して共通集合 $H \cap K$ が有限であることである．$\mathbb{R}^n$ の離散部分群の典型的な例は $\mathbb{Z}^n$ である．これがほとんど唯 1 つのものであることを示すつもりである．

定理 1. H を $\mathbb{R}^n$ の離散部分群とする．このとき，H は（$\mathbb{Z}$-加群として）$\mathbb{R}$ 上 1 次独立な r 個のベクトルで生成される（従って $r \leq n$）．

証明　$\{e_1, \ldots, e_r\}$ を $\mathbb{R}$ 上 1 次独立な H の元の集合とする．ここで r は可能な限り大きいものとする（$r \leq n$ である）．

$$P = \{x \in \mathbb{R}^n | \ x = \sum_{i=1}^{r} \alpha_i e_i, \ 0 \leq \alpha_i \leq 1 \} \tag{1}$$

をこれらのベクトルで張られる平行体 (parallelotope) とする．明らかに，P はコンパクトで，従って $P \cap H$ は有限である．$x \in H$ をとる．集合 $\{e_1, \ldots, e_r\}$ の極大性により，$x = \sum_{i=1}^{r} \lambda_i e_i, \ \lambda_i \in \mathbb{R}$ と書ける．$j \in \mathbb{Z}$ に対して，

$$x_j = jx - \sum_{i=1}^{r} [j\lambda_i] e_i \tag{2}$$

とおく（ここで，$[\mu]$ は $\mu \in \mathbb{R}$ 以下の最大の整数を表す Gauss の記号）．よって

$$x_j = \sum_{i=1}^{r} (j\lambda_i - [j\lambda_i]) e_i$$

であり，これより $x_j \in P$ となって，(2) から $x_j \in P \cap H$ となる．$x = x_1 + \sum_{i=1}^{r} [\lambda_i] e_i$ に注意すれば，$\mathbb{Z}$-加群 H は $P \cap H$ で生成され，よって有限型である．

一方，$P \cap H$ は有限で $\mathbb{Z}$ は無限であるから，異なる整数 j と k が存在して $x_j = x_k$ となる．(2) より $(j-k)\lambda_i = [j\lambda_i] - [k\lambda_i]$ で，これは λ_i がすべて有理数であることを示す．よって $\mathbb{Z}$-加群 H は係数が有理数である $\{e_i\}$ の 1 次結合の有限集合で生成される．d をこれらの係数の共通分母（$d \in \mathbb{Z} \setminus (0)$）とする．明らかに，$dH \subset \sum_{i=1}^{r} \mathbb{Z} e_i$ である．よって $\mathbb{Z}$-加群 $\sum_{i=1}^{r} \mathbb{Z} e_i$ の基底 $\{f_i\}$ と整数 α_i が存在して，$\{\alpha_1 f_1, \ldots, \alpha_r f_r\}$ が dH を生成する（1.5 節定理 1）．$\mathbb{Z}$-加群 dH は H と同じ階数をもち，$H \supset \sum_{i=1}^{r} \mathbb{Z} e_i$ であるから，dH の階数 $\geq r$ である．従って，dH の階数は r に等しく，すべての α_i は 0 ではない．よって，$\{e_i\}$ と同じように $\{f_i\}$ は $\mathbb{R}$ 上 1 次独立であることがわかる．加群 dH，つまり H は $\mathbb{R}$ 上 1 次独立な r 個のベクトルで（$\mathbb{Z}$ 上）生成される．　□

前述のことについての 1 つの応用

$t = (\theta_1, \ldots, \theta_n) \in \mathbb{R}^n$ を θ_i の中で少なくとも 1 つは無理数であるものとする．$\mathbb{R}^n$ の標準的な基底を $\{e_1, \ldots, e_n\}$ と書き，H を $\{e_1, \ldots, e_n, t\}$ で生成された $\mathbb{R}^n$ の部分群とすると，この H は離散的でない．なぜならば，もしそうでないとすると，定理 1 の証明の中で用いた方法によって，t は有理係数の $\{e_i\}$ の 1 次結合で表されることになり，不合理であるからである．従って，任意の $\varepsilon > 0$ に対して，0 と異なる H の元で 0 からの距離が ε より小さいものが存在する．よって，整数 $p_i \in \mathbb{Z}, q \in \mathbb{N}, q \neq 0$ で $|q\theta_i - p_i| \leq \varepsilon$ となるものがある．これは，すべての $i = 1, \ldots, n$ について

$$\left| \theta_i - \frac{p_i}{q} \right| \leq \frac{\varepsilon}{q}$$

が成り立つことを意味する．$1/q$ の整数倍 n_i/q で θ_i に最も近いものをとることにより，

$$\left|\theta_i - \frac{n_i}{q}\right| \leq \frac{1}{2q} \qquad (n_i \in \mathbb{Z})$$

という，より単純な近似を得る．これが任意の q について成り立つことに注意する．この結果は，無理数を有理数で近似するという数ある理論における基礎的な定理である．この分野についてより多くのことを知りたい読者は，Koksma, *Diophantische Approximation*, Berlin (Springer), 1936 を参考にしたらよいだろう．

定義 1. $\mathbb{R}^n$ の階数 n の離散部分群を $\mathbb{R}^n$ における**格子** (lattice) という．

定理 1 より，格子は $\mathbb{R}^n$ の基底によって $\mathbb{Z}$ 上生成される．その基底はさらに与えられた格子の $\mathbb{Z}$-基底である．格子 H の各 $\mathbb{Z}$-基底 $e = \{e_1, \ldots, e_n\}$ に対して半開平行体を P_e と書こう，すなわち

$$P_e = \{x \in \mathbb{R}^n \mid x = \sum_{i=1}^{n} \alpha_i e_i,\ \ 0 \leq \alpha_i < 1\}$$

とする．すべての $\mathbb{R}^n$ の点は H を法として P_e の唯 1 つの点と共役である（この場合に，P_e は H の**基本領域** (fundamental domain) という）．μ は Lebesgue 測度 (Lebesgue measure) を表す，すなわち，S を $\mathbb{R}^n$ の可測部分集合とするとき，$\mu(S)$ はその測度（その**体積** (volume) ともいう）を表そう．

補題 1. 体積 $\mu(P_e)$ は H の基底 e のとり方によらない．

証明 $f = \{f_1, \ldots, f_n\}$ を H の他の基底とする．このとき，

$$f_i = \sum_{j=1}^{n} \alpha_{ij} e_j \qquad (\alpha_{ij} \in \mathbb{Z})$$

と書ける．計算により $\mu(P_f) = |\det(\alpha_{ij})|\ \mu(P_e)$ を得る．行列 (α_{ij})（基底の変換に関するもの）は整数成分をもつ逆行列をもつ，可逆なものである．よって $\det(\alpha_{ij}) = \pm 1$．ゆえに $\mu(P_f) = \mu(P_e)$ となる． □

H の基底 e に付随した平行体 P_e の体積は**格子 H の体積**といわれ，$v(H)$ と

記される（「体積」という語がここでは乱用されている．なぜならば $\mu(H)=0$ であるからである．たぶん，格子 H の「網」(mesh) といった方がいいのではないだろうか）．

定理 2 (Minkowski). H を $\mathbb{R}^n$ の格子，S を可測な $\mathbb{R}^n$ の部分集合で $\mu(S) > v(H)$ であるものとする．このとき，異なる 2 点 $x, y \in S$ が存在して $x - y \in H$ が成り立つ．

証明　$e = \{e_1, \dots, e_n\}$ を H の $\mathbb{Z}$-基底とし，P_e を e に付随した平行体とする．P_e は H の基本領域であることより，S は共通部分をもたない部分集合 $S \cap (h + P_e)$　$(h \in H)$ の和集合である．よって，

$$\mu(S) = \sum_{h \in H} \mu(S \cap (h + P_e)) \tag{3}$$

となる．μ は平行移動について不変であるから

$$\mu(S \cap (h + P_e)) = \mu((-h + S) \cap P_e).$$

集合 $(-h + S) \cap P_e$　$(h \in H)$ がどの 2 つもすべて共通部分をもたないということはありえない．さもないと，$\mu(P_e) \geq \sum_{h \in H} \mu((-h + S) \cap P_e)$ となって，(3) と仮定 $\mu(P_e) = v(H) < \mu(S)$ に矛盾する．従って，異なる元 $h, h' \in H$ があって，$P_e \cap (-h + S) \cap (-h' + S) \neq \emptyset$ となる．x, y を S の元で $-h + x = -h' + y$ となるものとする．このとき，$x - y = h - h' \in H$ で，$h \neq h'$ より $x \neq y$ となる．□

系．H を $\mathbb{R}^n$ での格子，S を $\mathbb{R}^n$ の可測部分集合で原点 0 に関して対称的で凸形であるとする．S は次の 2 つの条件のうちの少なくとも 1 つはみたすとする．

(a) $\mu(S) > 2^n v(H)$

または

(b) $\mu(S) \geq 2^n v(H)$ かつ S はコンパクト．

このとき，$S \cap (H \setminus \{0\}) \neq \emptyset$ である．

証明 (a) の場合は定理 1 を集合 $S' = \frac{1}{2}S$ （$\mu(S') = 2^{-n}\mu(S) > v(H)$ であるから）に適用する．y, z を S' の異なる点で $y - z \in H$ となるものとする．このとき，$y - z = \frac{1}{2}(2y + (-2z))$ で S は対称性をもつ凸形であることより，$y - z$ は S にも属する．従って $y - z \in S \cap (H \setminus \{0\})$ となる．

(b) の場合も系の結論が成り立つことを示すために，(a) の場合を $(1 + \varepsilon)S$ ($\varepsilon > 0$) に適用する．そのとき $(H \setminus \{0\}) \cap (1 + \varepsilon)S$ は空でないコンパクトな集合である（これはコンパクトで離散であるから，有限でもある）．さらに $\bigcap_{\varepsilon > 0}(H \setminus \{0\}) \cap (1 + \varepsilon)S \neq \emptyset$ となる（なぜならば，空でない縮小されていくコンパクト集合の共通集合は決して空にならないからである）．これは $H \setminus \{0\}$ の点ですべての $\varepsilon > 0$ に対して $(1 + \varepsilon)S$ に属するものが存在することを意味する．従って，S がコンパクトであるから，その点は S にも属している． □

∞ (b) において，コンパクトであるという仮定は必要である．コンパクトでないとしたときの (b) に対する反例として，開平行体

$$\{x \in \mathbb{R}^n \mid x = \sum_{i=1}^{n} \lambda_i e_i, -1 < \lambda_i < 1\}$$

が考えられる．ここで $e = \{e_1, \ldots, e_n\}$ は基底で，e を $\mathbb{Z}$-基底としてもつ格子の下で作られる．

4.2 数体の標準的埋め込み

K を数体，n をその次数とする．(2.4 節定理 1 において）n 個の異なる同型（中への）$\sigma_i : K \to \mathbb{C}$ が存在することはすでに知っている．K の $\mathbb{Q}$ 上の原始元の最小多項式は $\mathbb{C}$ の中で n 個の根しか もたない（同上，定理 1 の系）から，ちょうど n 個である．$\alpha : \mathbb{C} \to \mathbb{C}$ を複素共役をとる写像とする．このとき，任意の $i = 1, \ldots, n$ に対して，ある j ($1 \leq j \leq n$) があって $\alpha \cdot \sigma_i = \sigma_j$ となり，また $\alpha \cdot \sigma_i = \sigma_i$ となるときの必要十分条件は $\sigma_i(K) \subset \mathbb{R}$ である．r_1 で $\sigma_i(K) \subset \mathbb{R}$ となる i の個数を表す．すると残りの $n - r_1$ は偶数なので，

$$r_1 + 2r_2 = n \tag{1}$$

と書ける．

σ_i の番号をつけかえて，$\sigma_i(K) \subset \mathbb{R}$ $(1 \leq i \leq r_1)$ で $\sigma_{j+r_2}(x) = \overline{\sigma_j(x)}$ $(r_1+1 \leq j \leq r_1+r_2)$ とする．このとき最初の r_1+r_2 個の同型 σ_i から残りの r_2 個が決定される．$x \in K$ に対して

$$\sigma(x) = (\sigma_1(x), \ldots, \sigma_{r_1+r_2}(x)) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \tag{2}$$

と定義する．σ は K の $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ への**標準的埋め込み** (canonical imbedding) とよばれる．これは単射環準同型である．しばしば $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ と $\mathbb{R}^n$ ((1) を参照) を同一視する．この章では以後これらの記号 σ, K, n, r_1, r_2 を使うことにする．

命題 1. M を階数 n の K の自由 $\mathbb{Z}$-部分加群，$\{x_i\}_{1\leq i\leq n}$ を M の $\mathbb{Z}$-基底とすると，$\sigma(M)$ は $\mathbb{R}^n$ の格子で，その体積は

$$v(\sigma(M)) = 2^{-r_2} \left| \det_{1\leq i,j\leq n}(\sigma_i(x_j)) \right| \tag{3}$$

である．

証明　i を固定したとき，$\sigma(x_i)$ の $\mathbb{R}^n$ の標準基底に関する成分は

$$\begin{aligned}\sigma_1(x_i), \ldots, \sigma_{r_1}(x_i),\ R(\sigma_{r_1+1}(x_i)),\ I(\sigma_{r_1+1}(x_i)),\ \ldots, \\ R(\sigma_{r_1+r_2}(x_i)),\ I(\sigma_{r_1+r_2}(x_i))\end{aligned} \tag{4}$$

である．ここで，R と I はそれぞれ実部と虚部を表す．i 列が (4) で与えられる行列の行列式 D を計算する．$z \in \mathbb{C}$ に対して，公式 $R(z) = \frac{1}{2}(z+\overline{z})$, $I(z) = \frac{1}{2i}(z-\overline{z})$ が成り立つことと，R と I は線型であることより，$D = (2i)^{-r_2}\det(\sigma_j(x_i))$ を得る．$\{x_i\}$ は K の $\mathbb{Q}$ 上の基底となるから，$\det(\sigma_j(x_i)) \neq 0$（2.7 節命題 3）で，よって $D \neq 0$ となる．従ってベクトル $\sigma(x_i)$ $(1 \leq i \leq n)$ は $\mathbb{R}^n$ の中で 1 次独立である．よって，それらが生成する $\mathbb{Z}$-加群（それが $\sigma(M)$）は $\mathbb{R}^n$ の格子である．上で行った D の計算により (3) が $\sigma(M)$ の体積を与えることが示される．□

命題 2. d を K の絶対判別式，A を K における整数環，$\mathfrak{a}$ を (0) でない A の整イデアルとする．このとき $\sigma(A)$ と $\sigma(\mathfrak{a})$ は格子である．さらに

$$v(\sigma(A)) = 2^{-r_2}|d|^{\frac{1}{2}}, \qquad v(\sigma(\mathfrak{a})) = 2^{-r_2}|d|^{\frac{1}{2}}\mathrm{N}(\mathfrak{a}) \tag{5}$$

が成り立つ.

証明 A と $\mathfrak{a}$ は階数 n の自由 $\mathbb{Z}$-加群である. よって命題 1 を適用できる. 一方, $\{x_i\}$ を A の $\mathbb{Z}$-基底とすれば, $d = \det(\sigma_i(x_j))^2$ (2.7 節命題 3) である. これより (5) の最初の公式が示される. 第 2 の公式は, 第 1 の公式と $\sigma(\mathfrak{a})$ が指数が $\mathrm{N}(\mathfrak{a})$ (3.5 節定義 1) である $\sigma(A)$ の部分群であることから出る. $\sigma(\mathfrak{a})$ の基本領域は, 明らかに, $\sigma(A)$ の基本領域を共通部分なく $N(\mathfrak{a})$ 回加えた和集合として構成される. □

4.3 イデアル類群の有限性

命題 1. K を数体, n をその次数, r_1 と r_2 を 4.2 節のはじめに定義したもの, d を K の絶対判別式, $\mathfrak{a}$ を K の (0) でない整イデアルとする. このとき, $\mathfrak{a}$ は 0 でない元 x で

$$|\mathrm{N}_{K/\mathbb{Q}}(x)| \le \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}|d|^{\frac{1}{2}}\mathrm{N}(\mathfrak{a}) \tag{1}$$

をみたすものを含む.

証明 σ を K の $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ への標準的埋め込み (4.2 節) とする. t を正の実数, B_t を元 $(y_1, \ldots, y_{r_1}, z_1, \ldots, z_{r_2}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ で

$$\sum_{i=1}^{r_1} |y_i| + 2\sum_{j=1}^{r_2} |z_j| \le t \tag{2}$$

をみたすもの全体の集合とする. このとき B_t はコンパクトかつ凸形で, 原点 $O \in \mathbb{R}^n$ に関して対称な集合である. この章の付録で与えられる計算により,

$$\mu(B_t) = 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2}\frac{t^n}{n!} \tag{3}$$

がわかる. いま, t を選んで $\mu(B_t) = 2^n v(\sigma(\mathfrak{a}))$, すなわち,

$$2^{r_1}\left(\frac{\pi}{2}\right)^{r_2}\frac{t^n}{n!} = 2^{n-r_2}|d|^{\frac{1}{2}}\mathrm{N}(\mathfrak{a}) \qquad \text{(4.2 節命題 2)}$$

あるいは，$t^n = 2^{n-r_1}\pi^{-r_2}n!|d|^{\frac{1}{2}}\mathrm{N}(\mathfrak{a})$ となるようにできる．

4.1 節の定理 2 の系より，ある 0 でない元 $x \in \mathfrak{a}$ が存在して $\sigma(x) \in B_t$ となる．そのノルムは絶対値

$$|\mathrm{N}(x)| = \prod_{i=1}^{r_1} |\sigma_i(x)| \prod_{j=r_1+1}^{r_1+r_2} |\sigma_j(x)|^2$$

である．相乗平均は相加平均を超えない（Hardy-Littlewood-Pólya, *Inequalities*, Cambridge University Press* を参照）から，(2) より

$$|\mathrm{N}(x)| \le \left(\frac{1}{n}\sum_{i=1}^{r_1}|\sigma_i(x)| + \frac{2}{n}\sum_{j=r_1+1}^{r_1+r_2}|\sigma_j(x)|\right)^n \le \frac{t^n}{n^n}$$

となる．結局，

$$|\mathrm{N}(x)| \le \frac{1}{n^n}2^{n-r_1}\pi^{-r_2}n!|d|^{\frac{1}{2}}\mathrm{N}(\mathfrak{a})$$

となり，この式と $r_1 + 2r_2 = n$ より (1) を得る．　□

系 1. 前と記号の下で，K の任意のイデアル類（3.4 節）は整イデアル $\mathfrak{b}$ で

$$\mathrm{N}(\mathfrak{b}) \le \left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}|d|^{\frac{1}{2}} \qquad (4)$$

をみたすものを含む．

証明　$\mathfrak{a}'$ を与えられた類のイデアルとする．$\mathfrak{a}'$ に単項イデアルを掛けることにより，$\mathfrak{a} = \mathfrak{a}'^{-1}$ は整イデアルであるとしてよい．(1) をみたす 0 でない元 $x \in \mathfrak{a}$ をとる．このとき，$\mathfrak{b} = x\mathfrak{a}^{-1}$ は整イデアルで $\mathfrak{a}'$ と同じ類に属する．ノルムの乗法性により $\mathrm{N}(\mathfrak{b})$ は (4) をみたす（3.5 節命題 2）．　□

系 2. K を数体，n をその次数，d をその絶対判別式とする．このとき，$n \ge 2$ に対して，

$$|d| \ge \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n-1}$$

* ［訳注］邦語版は G. H. ハーディ，J. E. リトルウッド，G. ポーヤ，不等式（細川尋史訳），シュプリンガー・フェアラーク東京，2003.

が成り立ち，$n/(\log|d|)$ は K に依存しない定数によりおさえられる．

証明 K の 0 でない整イデアル $\mathfrak{b}$ で $\mathrm{N}(\mathfrak{b}) \geq 1$ となるものが常に存在するので，(4) より $|d|^{\frac{1}{2}} \geq \left(\frac{\pi}{4}\right)^{r_2}\left(\frac{n^n}{n!}\right)$ となる．$\frac{\pi}{4} < 1$ かつ $2r_2 \leq n$ であることより $|d| \geq a_n$ がわかる．ここで $a_n = \left(\frac{\pi}{4}\right)^n \frac{n^{2n}}{(n!)^2}$ である．

そして $a_2 = \frac{\pi^2}{4}$，$\frac{a_{n+1}}{a_n} = \frac{\pi}{4}\left(1+\frac{1}{n}\right)^{2n} = \frac{\pi}{4}(1+2+(\text{正の項}))$ である（二項公式を用いた）ことがわかる．よって $a_{n+1}/a_n \geq (3\pi)/4$ である．従って $n \geq 2$ に対して

$$|d| \geq \frac{\pi^2}{4}\left(\frac{3\pi}{4}\right)^{n-2}$$

が成り立ち，この系の不等式がすぐ得られる．$n/\log|d|$ が一様におさえられることは，対数をとることによりわかる． □

定理 1 (Hermite-Minkowski). $\mathbb{Q}$ と異なる任意の数体 K に対して，K の絶対判別式 d は $\neq \pm 1$ である．

証明 系 2 を用いて，$|d| \geq \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n-1}$ がわかる．$\pi/3 > 1$, $3\pi/4 > 1$ であるから，$|d| > 1$ である． □

定理 2 (Dirichlet). 任意の数体 K について，イデアル類群は有限である（3.4 節）．

証明 命題 1 の系 1 によって，任意の正の整数 q に対して，q をノルムとしてもつ K の整イデアル $\mathfrak{b}$ 全体の集合が有限集合であることを示せばよい．そのようなイデアル $\mathfrak{b}$ に対して，$\mathrm{card}(A/\mathfrak{b}) = q$（3.5 節）である．任意の群について，元の位数は群の位数を割り切るから，$q \in \mathfrak{b}$ がいえる．よってイデアル $\mathfrak{b}$ は Aq を含んでいて，そのようなイデアル $\mathfrak{b}$ は高々有限個しかない（3.4 節公式 (8)，ないしは A/Aq の有限性による）． □

定理 3 (Hermite). $\mathbb{C}$ においては与えられた判別式 d をもつような数体は高々有限個しかない．

証明 命題 1 の系 2 より，そのような体の次数は有界である．ここで n と整

数 r_1, r_2 は固定されていると仮定してよい．K をそのような体とする．

$\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ において次の集合 B を考えよう．

(a) $r_1 > 0$ ならば，B は元 $(y_1, \ldots, y_{r_1}, z_1, \ldots, z_{r_2}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ で

$$\begin{aligned} |y_1| \leq 2^n \left(\frac{\pi}{2}\right)^{-r_2} |d|^{\frac{1}{2}}, \quad |y_i| \leq \frac{1}{2} \quad (i = 2, \ldots, r_1), \\ |z_j| \leq \frac{1}{2} \quad (j = 1, \ldots, r_2) \end{aligned} \tag{5}$$

をみたすものの全体とする．

(b) $r_1 = 0$ ならば，B は元 $(z_1, \ldots, z_{r_2}) \in \mathbb{C}^{r_2}$ で

$$\begin{aligned} |z_1 - \overline{z}_1| \leq 2^n \frac{8}{\pi} \left(\frac{\pi}{2}\right)^{-r_2} |d|^{\frac{1}{2}}, \quad |z_1 + \overline{z}_1| \leq \frac{1}{2}, \\ |z_j| \leq \frac{1}{2} \quad (j = 2, \ldots, r_2) \end{aligned} \tag{6}$$

をみたすものの全体である．

明らかに，B はコンパクトかつ凸形で，$\mathbb{R}^n$ の原点に関して対称的であり，体積は $2^{n-r_2}|d|^{\frac{1}{2}}$ となる†．σ を K の標準的埋め込み（4.2 節）とするとき，4.2 節の命題 2 と 4.1 節の定理 2 の系により，K の整数 $x(\neq 0)$ で $\sigma(x) \in B$ となるものを得る．

x が $\mathbb{Q}$ 上の原始的な K の元であることを示そう．(a) の場合，(5) は $|\sigma_i(x)| \leq 1/2$ $(i \neq 1)$ を示す．

$$|\mathrm{N}(x)| = \prod_{i=1}^{n} |\sigma_i(x)|$$

は正の整数（2.6 節命題 2 の系）であることより，$|\sigma_1(x)| \geq 1$ となり，任意の $i \neq 1$ に対して $\sigma_1(x) \neq \sigma_i(x)$ となる．しかしながら，もし x が原始的でないとすれば，$\sigma_1(x)$ はある $\sigma_i(x)$ $(i \neq 1)$ と一致してしまう（2.6 節命題 1）．(b) の場合は，同様にして $|\sigma_1(x)| = |\overline{\sigma_1(x)}| \geq 1$ となり，σ_j が σ_1 または $\overline{\sigma}_1$ でないときは $\sigma_1(x) \neq \sigma_j(x)$ となる．ところで，(6) は実数部分 $|R(\sigma_1(x))| \leq 1/4$ を示している．しかし，これは $\sigma_1(x)$ が実数ではありえないことを意味する．よって $\sigma_1(x) \neq \overline{\sigma_1(x)}$ である．(a) の場合のように，x は原始的であると結論がでる．

---

† B は (b) の場合，区間の積と円板の積と長方形の積であることを利用して計算できる．

公式 (5) と (6) は x の共役 $\sigma_i(x)$ の絶対値が有界であることを示している．従って $\sigma_i(x)$ についての基本対称式もまた絶対値が有界である．言い換えれば，x の最小多項式は，次数のみならず係数も絶対値が有界である．x は整数であるから，その最小多項式は最高次の係数が 1 で，係数がすべて $\mathbb{Z}$ に含まれている（2.6 節命題 2 の系）．x の最小多項式の次数と係数の絶対値が有界なので，x の最小多項式のとり方の可能性は高々有限個しかない．したがって $x \in \mathbb{C}$ の値も高々有限個の可能性しかない．x は K を生成するから，K のとり方の可能性は高々有限個しかありえない． □

4.4 単数定理

K を数体，A を K における整数環とする．ことばの使い方として，環 A における単元を「K の単数」と表現する．任意の環において，単元は乗法に関して群をなすことを思い出そう．A^* で A における単元のなす群を表す．

次の結果は有益である．

命題 1. K を数体，$x \in K$ とする．x が K の単数であるためには，x が K の整数でノルムが ± 1 であることが必要十分である．

証明 x を K の単数とすれば，$\mathrm{N}(x)$ と $\mathrm{N}(x^{-1})$ は $\mathbb{Z}$ に属する．よって $\mathrm{N}(x) \cdot \mathrm{N}(x^{-1}) = \mathrm{N}(xx^{-1}) = 1$ で，$\mathrm{N}(x) = \pm 1$ となる．逆に，x を K の整数でノルムが ± 1 のものとする．特性方程式は

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x \pm 1 = 0$$

$(a_i \in \mathbb{Z})$（2.6 節）の形になる．よって $\pm(x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1) = x^{-1}$ である．そして x^{-1} が K の整数であることより，x は単数である． □

定理 1 (Dirichlet). K を数体，n をその次数，r_1, r_2 を 4.2 節で定義された整数とする．$r = r_1 + r_2 - 1$ とおく．K の単数の群 A^* は $\mathbb{Z}^r \times G$ と同型になる．ここで，G は K に属する 1 のべき根全体からなる有限巡回群である．

証明　まず，A^* が有限型の可換群であることを示す．そして，その階数を計算しよう．

K から $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ への標準的埋め込み（4.2 節）

$$x \mapsto (\sigma_1(x), \ldots, \sigma_{r_1+r_2}(x))$$

と K^* から $\mathbb{R}^{r_1+r_2}$ への写像

$$x \mapsto L(x) = (\log|\sigma_1(x)|, \ldots, \log|\sigma_{r_1+r_2}(x)|) \tag{1}$$

を考える．(1) は準同型（すなわち，$L(xy) = L(x) + L(y)$）であり，K^* の**対数的埋め込み** (logarithmic imbedding) といわれる．B を $\mathbb{R}^{r_1+r_2}$ のコンパクトな部分集合とする．$L(x) \in B$ となる単数 $x \in A^*$ の集合 B' が有限集合であることを示す．実際，B は有界であるから，実数 $\alpha > 1$ があって任意の $x \in B'$ に対して $\alpha^{-1} \leq |\sigma_i(x)| \leq \alpha$ $(i = 1, \ldots, n)$ となる．これより，$\sigma_i(x)$ の基本対称式は絶対値をとると有界である．$x \in A$ よりそれらは $\mathbb{Z}$ に属するから，$\sigma_i(x)$ の対称式の値をとる集合は有限集合である．従って，$x \in B'$ の特性多項式は高々有限個しかない．その結果，x のとれる値も高々有限個しかない．ゆえに B' は有限集合である．

B' の有限性より直ちに次のことが導かれる．

(a)　L を A^* に制限したときの核 G は有限群である．従ってそれは 1 のべき根からなり，巡回群である（1.6 節定理 1）．明らかに，K における 1 のべき根はすべて L の核に属する．なぜならば，K における 1 のべき根は整数であり，もし x が K の 1 のべき根とすれば，$|\sigma_i(x)|^q = |\sigma_i(x^q)| = |1| = 1$ となり，任意の i に対して $|\sigma_i(x)| = 1$ となるからである．

(b)　像 $L(A^*)$ は $\mathbb{R}^{r_1+r_2}$ の離散部分群である（4.1 節）．よって $L(A^*)$ は自由 $\mathbb{Z}$-加群で階数 $s \leq r_1 + r_2$　（4.1 節定理 1）である．$L(A^*)$ は自由加群であるから，A^* は $G \times L(A^*) = G \times \mathbb{Z}^s$ と同型である．$L(A^*)$ の階数 s が $r_1 + r_2 - 1$ に等しいことを示すことが残っている．

不等式 $s \leq r_1 + r_2 - 1$ は容易にわかる．実際，$x \in A^*$ に対して関係式

$$\pm 1 = \mathrm{N}(x) = \prod_{i=1}^{n} \sigma_i(x) = \prod_{i=1}^{r_1} \sigma_i(x) \prod_{j=r_1+1}^{r_1+r_2} \sigma_j(x)\overline{\sigma_j(x)} \quad \text{（命題 1）}$$

は，ベクトル $L(x) = (y_1, \ldots, y_{r_1+r_2})$ が次の式

$$\sum_{i=1}^{r_1} y_i + 2 \sum_{j=r_1+1}^{r_1+r_2} y_j = 0 \tag{2}$$

で定義される超平面 W の中にあることを示している．$L(A^*)$ は W の離散部分群であるから，$s \leq r_1 + r_2 - 1$ である．

さて，$L(A^*)$ が $r = r_1 + r_2 - 1$ 個の 1 次独立なベクトルを含むことを示そう．これにはよりデリケートな議論が求められる．このことを示すには，W 上の任意の 1 次形式 $f \neq 0$ に対して単数 u が存在して $f(L(u)) \neq 0$ であることを示せばよい．W から $\mathbb{R}^r$ への射影は（(2) によって）同型であるから，任意の $y = (y_1, \ldots, y_{r+1}) \in W \subset \mathbb{R}^{r+1}$ に対して

$$f(y) = c_1 y_1 + \cdots + c_r y_r \qquad (c_i \in \mathbb{R}) \tag{3}$$

と書いてもよい．

$$\alpha \geq 2^n \left(\frac{1}{2\pi}\right)^{r_2} |d|^{\frac{1}{2}}$$

となる実数 α をとめておく．任意の r 個の正の実数からなる組 $\lambda = (\lambda_1, \ldots, \lambda_r)$ に対して，実数 $\lambda_{r+1} > 0$ を $\prod_{i=1}^{r_1} \lambda_i \prod_{j=r_1+1}^{r_1+r_2} \lambda_j^2 = \alpha$ となるようにとる．いま，$\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ において，元 $(y_1, \ldots, y_{r_1}, z_1, \ldots, z_{r_2})$ $(y_i \in \mathbb{R}, z_j \in \mathbb{C})$ で $|y_i| \leq \lambda_i$，$|z_j| \leq \lambda_{j+r_1}$ となるもの全体の集合を B とすれば，これはコンパクトかつ凸形，原点 O に関して対称的で，体積は $\prod_{i=1}^{r_1} 2\lambda_i \prod_{j=r_1+1}^{r_2+r_1} \pi\lambda_j^2 = 2^{r_1}\pi^{r_2}\alpha \geq 2^{n-r_2}|d|^{\frac{1}{2}}$ である．従って 4.2 節の命題 2 と 4.1 節の定理 2 の系により，整数 $x_\lambda \in K$ で $\sigma(x_\lambda) \in B$ となるものが存在する．これは $|\sigma_i(x_\lambda)| \leq \lambda_i$ $(i = 1, \ldots, n)$（ここで $\lambda_{j+r_2} = \lambda_j$，$j = r_1+1, \ldots, r_1+r_2$）を意味する．$x_\lambda$ は整数であるから，

$$1 \leq |\mathrm{N}(x_\lambda)| = \prod_{i=1}^{n} |\sigma_i(x_\lambda)| \leq \prod_{i=1}^{r_1} \lambda_i \prod_{j=r_1+1}^{r_1+r_2} \lambda_j^2 = \alpha$$

となる．他方，任意の i について，

$$|\sigma_i(x_\lambda)| = |\mathrm{N}(x_\lambda)| \prod_{j \neq i} |\sigma_j(x_\lambda)|^{-1} \geq \prod_{j \neq i} \lambda_j^{-1} = \lambda_i \alpha^{-1}$$

である．ここで，任意の i に対して $\lambda_i \alpha^{-1} \leq |\sigma_i(x_\lambda)| \leq \lambda_i$ なので，

$$0 \leq \log \lambda_i - \log |\sigma_i(x\lambda)| \leq \log \alpha \tag{4}$$

となる．(3) を用いて

$$\left| f(L(x_\lambda)) - \sum_{i=1}^{r} c_i \log \lambda_i \right| \leq \left(\sum_{i=1}^{r} |c_i| \right) \log \alpha \qquad (5)$$

を得る．β を (5) の右辺より真に大きい定数とする．任意の正の整数 h に対して，r 個の正の実数 $\lambda_{i,h}$ $(i = 1, \ldots, r)$ で $\sum_{i=1}^{r} c_i \log \lambda_{i,h} = 2\beta h$ となるものを選ぶ．

$$\lambda(h) = (\lambda_{1,h}, \ldots, \lambda_{r,h})$$

とおいて，x_h を $x_{\lambda(h)}$ に対応する整数とする．(5) により

$$|f(L(x_h)) - 2\beta h| < \beta$$

なので，

$$(2h-1)\beta < f(L(x_h)) < (2h+1)\beta \qquad (6)$$

を得る．よって (6) より数 $f(L(x_h))$ はすべて異なる．他方，$|\mathrm{N}(x_h)| \leq \alpha$ であるから，Ax_h の形のイデアルで異なるものの数は高々有限である（4.3 節定理 2 の証明を参照）．従って 2 つの異なる添字 h, k が存在して $Ax_h = Ax_k$ となる．よって単数 $u \in A$ があって $x_k = ux_h$ となる．(f は線型であるから）$f(L(u)) = f(L(x_k)) - f(L(x_h)) \neq 0$ という結論がでる． □

注意．定理 1（「単数定理」とよばれる）は $r(= r_1 + r_2 - 1)$ 個の K の単数 $\{u_i\}$ が存在して，K の任意の単数 u は一意的に

$$u = zu_1^{n_1} \cdots u_r^{n_r} \qquad (7)$$

（$n_i \in \mathbb{Z}$, z は 1 のべき根）の形に書けることを示している．集合 $\{u_1, \ldots, u_r\}$ は K の単数の**基本系** (fundamental system)（**基本単数系**）といわれる．

例（円分体）．p を奇素数，z を 1 の原始複素 p 乗根，K を円分体 (cyclotomic field) $\mathbb{Q}[z]$ とする（2.9 節を参照）．このとき，$[K : \mathbb{Q}] = p - 1$（同上，定理 1）．$\mathbb{C}$ において z の共役は実数でないから，$r_1 = 0$ で，$2r_2 = p - 1$．よって $r = (p-3)/2$ となる．

4.5　虚 2 次体の単数

K を虚 2 次体（2.5 節）とする．このとき，$r_1 = 0$, $2r_2 = 2$ で $r_2 = 1$, $r_1 + r_2 - 1 = 0$ である．従って K における単数は K に含まれる 1 のべき根のみである（4.4 節定理 1）．それは有限巡回群をなす．少し計算をすることによって，この結果を直接証明し，結果をより精密にしよう．

m を平方因子をもたない正の整数として，$K = \mathbb{Q}[\sqrt{-m}]$ とおく．K の単数はノルムが ± 1 であった（4.4 節命題 1）．

(1)　$m \equiv 1$ または $2 \pmod 4$ であれば，K の整数環は $\mathbb{Z} + \mathbb{Z}\sqrt{-m}$ である（2.5 節定理 1）．$x = a + b\sqrt{-m}$ $(a, b \in \mathbb{Z})$ に対して，

$$\mathrm{N}(x) = a^2 + mb^2 \geq 0$$

である．x が単数であるためには，$a^2 + mb^2 = 1$ でなければならない．もし $m \geq 2$ ならば，これは $b = 0$, $a = \pm 1$ を意味し，よって $x = \pm 1$ である．もし $m = 1$ ならば，解 $x = \pm 1$ に加えて，解 $a = 0$, $b = \pm 1$ すなわち $x = \pm i$（ここで $i^2 = -1$）がある．

(2)　$m \equiv 3 \pmod 4$ であれば，K の整数環は $\mathbb{Z} + \mathbb{Z}[(1 + \sqrt{-m})/2]$ である（2.5 節定理 1）．$x = a + \frac{b}{2}(1 + \sqrt{-m})$ $(a, b \in \mathbb{Z})$ に対して，$\mathrm{N}(x) = (a + \frac{b}{2})^2 + \frac{mb^2}{4}$ を得る．x が単数であるためには，$(2a + b)^2 + mb^2 = 4$ でなければならない．もし $m \geq 7$ ならば，これは $b = 0$ を意味していて，$(2a)^2 = 4$, $a = \pm 1$ となり，$x = \pm 1$ となる．もし $m = 3$ ならば，$b = \pm 1$, $(2a \pm 1)^2 = \pm 1$ という関係より，解として

$$x = \frac{1}{2}(\pm 1 \pm \sqrt{-3})$$

がさらに付け加わることになる（符号 $\pm$ は同順とは限らない）．

まとめると，次の結果を証明したことになる．

命題 1.　K を虚 2 次体とする．次の 2 つの場合を除いて，K の単数群 G は 1 の平方根 $+1$ と -1 からなる．

(1)　$K = \mathbb{Q}[i]$ $(i^2 = -1)$ のとき，G は 1 の 4 乗根，すなわち，$i, -1, -i, 1$ からなる．

(2) $K=\mathbb{Q}[\sqrt{-3}]$ のとき，G は 1 の 6 乗根，すなわち，$\left(\frac{1+\sqrt{-3}}{2}\right)^j$ $(j=0,1,\ldots,5)$ からなる．

4.6　実 2 次体の単数

この節は前節に比べてかなり興味深いものになるはずである．K を実 2 次体とする．いつもの記号を用いて $r_1=2, r_2=0$ となり，よって $r=r_1+r_2-1=1$ である．単数定理（4.4 節定理 1）は，K の単数群が $\mathbb{Z}$ と K に含まれる 1 のべき根の群との積と同型であることを述べている．K は $\mathbb{R}$ の中へ埋め込めるから，1 のべき根は ± 1 のみである．よって，K を $\mathbb{R}$ の中に埋め込むことにして，次の命題を得る．

命題 1. 実 2 次体 $K\subset\mathbb{R}$ の正の単数は（加法群）$\mathbb{Z}$ と同型な（乗法的）群をなす．

この群は 1 より大きい生成元を唯 1 つ含んでいる．それは K の**基本単数** (fundamental unit) といわれる．

証明　$d\geq 2$ を平方因子をもたない整数として，$K=\mathbb{Q}[\sqrt{d}]$ とおき，$x=a+b\sqrt{d}$ $(a,b\in\mathbb{Q})$ を K の単数とする．$x, x^{-1}, -x, -x^{-1}$ は K の単数で，$\mathrm{N}(x)=(a+b\sqrt{d})(a-b\sqrt{d})=\pm 1$（4.4 節命題 1）であるから，これらの 4 つの数は $\pm a\pm b\sqrt{d}$ である．$x\neq\pm 1$ に対して $x, x^{-1}, -x, -x^{-1}$ の 4 つの数のうち唯 1 つのみが 1 より大きい．そしてそれは 4 つの中で最大のものである．よって K の 1 より大きい単数は $a+b\sqrt{d}$ $(a>0, b>0)$ の形のものである．

(a)　まず $d\equiv 2$ または $3 \pmod 4$ とする．このとき，K の整数環は $\mathbb{Z}+\mathbb{Z}\sqrt{d}$ である（2.5 節定理 1）．K の単数はノルム ± 1 の整数であるから（4.4 節命題 1），K の 1 より大きい単数は $a+b\sqrt{d}$, $a,b\in\mathbb{Z}$, $a>0, b>0$ で

$$a^2-db^2=\pm 1 \tag{1}$$

をみたす．

(1) の「自然数における」解 (a,b) (「Pell-Fermat の方程式」) は次のようにして得られる，すなわち，まず K の基本単数 $a_1+b_1\sqrt{d}$ をとり，

$$a_n+b_n\sqrt{d}=(a_1+b_1\sqrt{d})^n \quad (n\geq 1) \tag{2}$$

とおく．列 (a_n,b_n) は (1) のすべての解を表す．

☞ **注意**．i) (2) より $b_{n+1}=a_1b_n+b_1a_n$ を得る．a_1,b_1,a_n,b_n はすべて正であるから，列 (b_n) は真の増大列である．よって基本単数 $a_1+b_1\sqrt{d}$ を明確に計算するためには，列 (db^2) $(b\in\mathbb{N}, b\geq 1)$ を書き出し，この列で平方 a_1^2 と ± 1 だけ異なる最初の数 db_1^2 のところで止める．このとき $a_1+b_1\sqrt{d}$ は K の基本単数になる．たとえば，もし $d=7$ ならば，列 (db^2) は $7, 28, 63=64-1=8^2-1$ となるから，$b_1=3, a_1=8$ ととることによって，$8+3\sqrt{7}$ が $\mathbb{Q}[\sqrt{7}]$ の基本単数であることがわかる．同様にして，$\mathbb{Q}[\sqrt{2}], \mathbb{Q}[\sqrt{3}], \mathbb{Q}[\sqrt{6}]$ の基本単数はそれぞれ，$1+\sqrt{2}, 2+\sqrt{3}, 5+2\sqrt{6}$ であることがわかる．連分数の理論を用いれば，基本単数の計算についてほかのもっと素早い手順を見いだすことができる．

ii) 基本単数がノルム 1 であるならば，列 (a_n,b_n) は方程式 $(1')$ $a^2-db^2=1$ についての解を与えるだけである．この場合，方程式 $(1'')$ $a^2-db^2=-1$ は自然数の中では解をもたない．もし基本単数がノルム -1 をもてば，$(1')$ の解は列 (a_{2n},b_{2n}) からなる．そして $(1'')$ の解は列 (a_{2n+1},b_{2n+1}) からなる．第 1 の場合は $d=3,6,7$ のときに起き，第 2 の場合は $d=2,10$ のときに起きる ($3+\sqrt{10}$ が $\mathbb{Q}[\sqrt{10}]$ における基本単数である)．

(b) さて，$d\equiv 1 \pmod 4$ とする．$K=\mathbb{Q}[\sqrt{d}]$ の整数は $\frac{1}{2}(a+b\sqrt{d})$，ここで $a,b\in\mathbb{Z}$ でこれらは同じ偶奇性をもつ (2.5 節定理 1)．従って，もし $\frac{1}{2}(a+b\sqrt{d})$ が K の単数ならば (4.4 節命題 2)，

$$a^2-db^2=\pm 4 \tag{3}$$

でなければならない．

逆に (a,b) が (3) の整数解であれば，$\frac{1}{2}(a+b\sqrt{d})$ は K の整数 (そのトレースは a で，そのノルムは (3) より ± 1) なので，K の単数である．(a) のときと同様に，K の基本単数を $a_1+b_1\sqrt{d}$ と書くと，(3) の自然数の組 (a,b) における解は次のように定義した列 (a_n,b_n) $(n\geq 1)$ の値となる．

$$a_n+b_n\sqrt{d}=2^{1-n}(a_1+b_1\sqrt{d})^n. \tag{4}$$

$a_1 + b_1\sqrt{d}$ の計算は (a) のときと同様にしてできる．たとえば，$\mathbb{Q}[\sqrt{5}]$, $\mathbb{Q}[\sqrt{13}]$, $\mathbb{Q}[\sqrt{17}]$ の基本単数は，それぞれ $\frac{1}{2}(1+\sqrt{5})$, $\frac{1}{2}(3+\sqrt{13})$, $4+\sqrt{17}$ である．これら 3 つの単数のノルムは -1 である．(3) において符号 ± 1 のとり方については，(a) で得られたとり方と同様な結果となる．□

注意．$d \equiv 1 \pmod 4$ の場合，Pell-Fermat の方程式

$$a^2 - db^2 = \pm 1 \tag{5}$$

の解は環 $B = \mathbb{Z}[\sqrt{d}]$ に属する単数 $a+b\sqrt{d}$ $(a, b > 0)$ と対応する．この環 B は K の整数環 A の部分環であり，B の正の単数は A の正の単数のなす群の部分群 G をなす．$u = \frac{1}{2}(a+b\sqrt{d})$ を K の基本単数とする．もし，a, b ともに偶数ならば，$u \in B$ で，G は u のべきからなる（これは，たとえば $d = 17$ のときにあてはまる）．もし a と b がともに奇数ならば，$u^3 \in B$ となる（このことを見るためには，$8u^3 = a(a^2+3b^2d) + b(3a^2+b^2d)\sqrt{d}$ に注意する．$a^2 - b^2d = \pm 4$ であるから，$a^2 + 3b^2d = 4(b^2d \pm 1)$ であり，b と d が奇数なのでこれは 8 の倍数である．同様にして $3a^2 + b^2d = 4(a^2 \pm 1)$ であり，a が奇数であるから，これもまた 8 の倍数になる）．この場合，G は u^3 のべきからなる（$u^2 \notin B$ である．そうでないと $u = u^3/u^2 \in B$ となってしまう）．これは，たとえば $d = 5$（ないしは $d = 13$）のときがそうで，その場合は $u^3 = 2 + \sqrt{5}$（ないしは $u^3 = 18 + 5\sqrt{13}$）である．

4.7　単数定理の一般化

命題 1． A を有限型の $\mathbb{Z}$-加群である環とする．このとき，A の単元全体からなる乗法群 A^* は有限型の（可換な）群である．

可換群 G が「有限型」であるというのは，「G を $\mathbb{Z}$-加群と見なして，その構造に関して有限型」であるということを意味する．有限型の可換群の部分群は有限型である（3.1 節定理 1 の系 2）．上の A のイデアルは A の $\mathbb{Z}$-部分加群であるから，A は Noether 環であることに注意する．

命題の証明． まず最初に A が整域のときを扱う．もしその分数体 K が標数 0 ならば，K は $\mathbb{Q}$ 上有限次元のベクトル空間であり，K は数体である．他方，A は（それが有限型の $\mathbb{Z}$-加群であるから）$\mathbb{Z}$ 上整である（2.1 節定理 1

を参照）．従って，A は K の整数環 B の部分環である．よって $A^* \subset B^*$ となり，B^* は単数定理（4.4 節定理 1）より有限型なので，A^* も有限型である．K が標数 $p \neq 0$ ならば，K は $\mathbb{F}_p$ の有限拡大で，K は有限体となり，A^* は有限群である．

さて，次は A が被約 (reduced) の場合（定義より，A のべき零元は 0 のみである）に移る．ここで次の補題が必要となる．

補題． A が被約な Noether 環ならば，イデアル (0) は有限個の素イデアルの共通部分として表される．

証明 Noether 環においては，任意のイデアルは素イデアルの積を含む（3.3 節補題 3）．(0) は最小のイデアルであるから，(0) は素イデアルの積である，すなわち $(0) = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_q^{n_q}$ となる．$x \in \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_q$ をとると，$x^{n_1+\cdots+n_q} \in \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_q^{n_q} = (0)$ となり，$x^{n_1+\cdots+n_q} = 0$ がわかる．A は被約であるから，$x = 0$ を意味する．ゆえに，$\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_q = (0)$ を得る． □

さて命題 1 の証明に戻る．$(0) = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_q$，ここで $\mathfrak{p}_i$ は素イデアルであるとする．標準的準同型 $\phi : A \to \prod_{i=1}^{q} A/\mathfrak{p}_i$ は単射となる．環の直積の元が可逆であるためにはその成分のすべてが可逆であることが必要十分であることより，$(\prod_i A/\mathfrak{p}_i)^* = \prod_i (A/\mathfrak{p}_i)^*$ である．整域の場合は，各 $(A/\mathfrak{p}_i)^*$ は有限型である．従って $\prod (A/\mathfrak{p}_i)^*$ は有限型であり，その任意の部分群，たとえば $\phi(A^*)$ もそうである（$\mathbb{Z}$ が Noether 環であったことに注意する）．ϕ は単射であるから，A^* は有限型となる．

最後に，一般の場合を考えよう．A のべき零元全体の集合 $\mathfrak{n}$ は A のイデアルである．なぜならば，$x^p = 0$, $y^q = 0$, $a \in A$ に対して，$(x+y)^{p+q-1} = 0, (ax)^p = 0$ が成り立つからである．一方，$\mathfrak{n}^s = (0)$ となる整数 s が存在する（これを見るために，$\{x_1, \ldots, x_r\}$ を Noether 環 A のイデアル $\mathfrak{n}$ の生成元からなる有限集合とする．$x_i^{q_i} = 0$ $(i = 1, \ldots, r)$ と仮定して，$s = q_1 + \cdots + q_r$ とすれば，$\mathfrak{n}^s = (0)$ は明らかである）．s の帰納法を用いる．$s = 1$ の場合は被約の場合なので，既に扱っている．$s > 1$ として，ϕ を標準的準同型 $\phi : A \to A/\mathfrak{n}^{s-1}$ とする．このとき，$\phi(A^*) \subset (A/\mathfrak{n}^{s-1})^*$ なので，$\phi(A^*)$ は有限型である．ϕ の核 (kernel) を A^* に制限すると $1 + \mathfrak{n}^{s-1}$ に含まれ

る．実際，$\mathrm{Ker}(\phi) \cap A^* = 1 + \mathfrak{n}^{s-1}$ となる．なぜならば，$s > 1$ に対して $(\mathfrak{n}^{s-1})^2 \subset \mathfrak{n}^s = (0)$ が成り立ち，これより任意の元 $1 + x \in 1 + \mathfrak{n}^{s-1}$ は $1 - x$ を逆元としてもつからである．実際，$(1+x)(1-x) = 1 - x^2 = 1$ である．$1 + \mathfrak{n}^{s-1}$ が有限型であることを示すことが残っている．ここで，A は有限型の $\mathbb{Z}$-加群であることより，A の部分加群 $\mathfrak{n}^{s-1}$ も有限型である．よって加法群 $\mathfrak{n}^{s-1}$ から（乗法群）$1 + \mathfrak{n}^{s-1}$ への写像 $x \mapsto 1 + x$ が同型であることを示せば十分である．ところが，$(\mathfrak{n}^{s-1})^2 = (0)$ であるから $(1+x)(1+y) = 1 + x + y$ $(x, y \in \mathfrak{n}^{s-1})$ が成り立つので，同型であることは明らかである．よって 3.1 節の命題 1 より A^* は有限型であることがわかる．□

∞ 代数幾何学から議論を借用してくると，任意の被約な環 $B = \mathbb{Z}[x_1, \ldots, x_n]$（すなわち，環として $\mathbb{Z}$ 上有限生成）について，B の単元全体のなす群 B^* は有限型である（[6]）ことが示せる．

付　録

体積の計算

命題．$r_1, r_2 \in \mathbb{N}, n = r_1 + 2r_2, t \in \mathbb{R}, B_t$ を元 $(y_1 \ldots, y_{r_1}, z_1, \ldots, z_{r_2}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ で

$$\sum_{i=1}^{r_1} |y_i| + 2\sum_{j=1}^{r_2} |z_j| \leq t \tag{1}$$

をみたすもの全体の集合とする．μ は $\mathbb{R}^n$ における Lebesgue 測度を表す．このとき，$\mu(B_t) = 0$ が任意の $t < 0$ に対して，

$$\mu(B_t) = 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{t^n}{n!} \tag{2}$$

が任意の $t \geq 0$ に対して成り立つ．

証明　$t < 0$ のとき $B_t = \emptyset$ かつ $\mu(B_t) = 0$ なので，$t \geq 0$ について考える．$\mu(B_t) = V(r_1, r_2, t)$ とおき，r_1 と r_2 の二重帰納法で証明する．明らかに $V(1, 0, t) = 2t$（線分 $[-t, t]$），$V(0, 1, t) = (\pi t^2)/4$（半径 $t/2$ の円）であ

る．これらの特別な場合は (2) をみたす．

いま，(2) の右辺が $V(r_1,r_2,t)$ となると仮定する．まず，$V(r_1+1,r_2,t)$ を計算しよう．集合 $B_t\subset\mathbb{R}\times\mathbb{R}^{r_1}\times\mathbb{C}^{r_2}$，これは r_1+1，r_2 に対応する，は関係

$$|y|+\sum_{i=1}^{r_1}|y_i|+2\sum_{j=1}^{r_2}|z_j|\le t \quad (y\in\mathbb{R})$$

で定義されている．($|y|>t$ ならば，$B_t=\emptyset$ に注意して) 積分を行うと，

$$V(r_1+1,r_2,t)=\int_{\mathbb{R}}V(r_1,r_2,t-|y|)dy=\int_{-t}^{+t}V(r_1,r_2,t-|y|)dy$$

を得る．帰納法の仮定により

$$V(r_1+1,r_2,t)=2\int_0^t 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2}\frac{(t-y)^n}{n!}dy=2^{r_1+1}\left(\frac{\pi}{2}\right)^{r_2}\frac{t^{n+1}}{(n+1)!}$$

を得る．これは (2) と一致する．

$V(r_1,r_2+1,t)$ の計算が残っている．$V(r_1,r_2,t)$ は (2) をみたすという帰納法の仮定はそのままにしておく．集合 $B_t\subset\mathbb{R}^{r_1}\times\mathbb{C}^{r_2}\times\mathbb{C}$（これは r_1,r_2+1 に対応する）は関係

$$\sum_{i=1}^{r_1}|y_i|+2\sum_{j=1}^{r_2}|z_j|+2|z|\le t \quad (z\in\mathbb{C})$$

で定義されている．再度積分を行うことにより

$$V(r_1,r_2+1,t)=\int_{\mathbb{C}}V(r_1,r_2,t-2|z|)d\mu(z)=\int_{|z|\le t/2}V(r_1,r_2,t-2|z|)d\mu(z)$$

を得る．ここで $d\mu(z)$ は $\mathbb{C}$ における Lebesgue 測度を表す．$z=\rho e^{i\theta}$ ($\rho\in\mathbb{R}_+,0\le\theta\le2\pi$) とおくと，$d\mu(z)=\rho d\rho d\theta$ である．帰納法の仮定により

$$\begin{aligned}V(r_1,r_2+1,t)&=\int_0^{t/2}\int_0^{2\pi}2^{r_1}\left(\frac{\pi}{2}\right)^{r_2}\frac{(t-2\rho)^n}{n!}\rho d\rho d\theta\\&=2^{r_1}\left(\frac{\pi}{2}\right)^{r_2}\frac{2\pi}{n!}\int_0^{t/2}(t-2\rho)^n\rho d\rho\end{aligned}$$

を得る．$2\rho=x$ とおいて一部分の積分を行うことにより $\int_0^{t/2}(t-2\rho)^n\rho d\rho$ を計算すると，これは $t^{n+2}/(4(n+1)(n+2))$ の値をもつ．従って

$$V(r_1, r_2+1, t) = 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2+1}\frac{t^{n+2}}{(n+2)!}$$

となり，$r_1 + 2(r_2+1) = n+2$ であるからこれは (2) と一致する．　□

練習問題

1*. 3 次体 $\mathbb{Q}[x]$, $x^3=2$, の整数環 A は単項イデアル環であることを示せ（ヒント：A の判別式を $D(1,x,x^2)$ でおさえて，4.3 節の命題 1 の系 1 を適用すると $A=\mathbb{Z}[x]$ である．巻末の演習問題を見よ）．

2*. 環 $A=\mathbb{Z}[X]/(X^3)$ の単元と群 A^* の構造を決定せよ．

3*. K を 3 次体で $r_1=r_2=1$ とする．K が $\mathbb{R}$ の中に埋め込まれていると仮定する．

(a) K の正の単数全体は $\mathbb{Z}$ と同型な群であること，K の正の単数はすべてノルムが 1 であることを示せ．

(b) d を K の絶対判別式，u を 1 より大きな単数とする．$|d|\leq 4u^3+24$ であることを示せ（ヒント：$u=x^2$ $(x\in\mathbb{R})$, $x>0$ とおくと，u の共役は $x^{-1}e^{iy}$ と $x^{-1}e^{-iy}(y\in\mathbb{R})$ の形であることに注意する．判別式 $d'=D(1,u,u^2)$ を x,y の関数として計算し，$|d'|^{1/2}=\varphi(x,y)$ とおく．x を固定したときの $\varphi(x,y)$ の最小値を見つけ，それより $|d'|\leq 4u^3+24$ を導く．d が d' を割り切ることを調べることにより結論を得る）．

(c) 多項式 $X^3+10X+1$ は $\mathbb{Q}$ 上既約であることを示せ（5.3 節の最後のあたりの例を参照）．x をその実根の 1 つとする．3 次体 $\mathbb{Q}[x]$ の整数環が $\mathbb{Z}[x]$ であることを示せ（ヒント：同上）．$u=-1/x$ は $\mathbb{Q}[x]$ の正の単数からなる群の生成元であることを示せ．

4*. K を数体，A を K の整数環，P を A の極大イデアル全体の集合とする．$\mathfrak{p}\in P$ と $x\in K^*$ に対して，$v_{\mathfrak{p}}(x)$ により Ax を素イデアルの積に分解したときの $\mathfrak{p}$ の指数を表す．$v_{\mathfrak{p}}(0)=+\infty$ とおく．

(a) $x,y\in K$ に対して，$v_{\mathfrak{p}}(xy)=v_{\mathfrak{p}}(x)+v_{\mathfrak{p}}(y)$ と $v_{\mathfrak{p}}(x+y)\geq\min(v_{\mathfrak{p}}(x),v_{\mathfrak{p}}(y))$ が成り立つことを示せ．

(b) $P'\subset P$ とする．すべての $\mathfrak{p}\in P'$ に対して $v_{\mathfrak{p}}(x)\geq 0$ となるような $x\in K$ の集合 $A(P')$ は K の部分環であることを示せ．$P'=P$ と $P'=\emptyset$ の場合を考えよ．

(c) P' として有限集合 $S\subset P$ の補集合をとる．$A(P')$ の単数の群 U は有限型で，U/A^* は階数が card(S) の自由 $\mathbb{Z}$-加群であることを示せ（ヒント：U から $\mathbb{Z}^s$ への写像 $x\mapsto(v_{\mathfrak{p}}(x))_{\mathfrak{p}\in S}$ を考える．そして，その核を見つける．次に A のすべてのイデアルが適当なべきをとると単項イデアルになることを調べることによって，その像を決定する）．

第 V 章　拡大体における素イデアルの分解

K を数体，A を K の整数環，L を K の有限拡大，B を A の L における整閉包（すなわち，L の整数環）とする．B において A の (0) でない素イデアル $\mathfrak{p}$ により生成されたイデアル $\mathfrak{p}B$ は一般には素イデアルではない．$\mathfrak{p}B$ は素イデアルの積に分解する（3.4 節定理 3），すなわち，$\mathfrak{p}B = \prod_i \mathfrak{P}_i^{e_i}$ となる．この章ではこの分解について調べてみることにする．B が自由 A-加群の場合（たとえば，A が単項イデアル環，2.7 節定理 1 の系を参照）は際だって簡単である．5.1 節においては一般の場合がどのようにしてこの簡単な場合に帰着するかを示すことにしよう．

5.1　分数環に関する準備

定義 1. A は整域，K をその分数体，S は $A \setminus (0)$ の部分集合で 1 を含み乗法に関して閉じている集合とする．K の元で a/s $(a \in A, s \in S)$ の形に書けるもの全体の集合を S に関する A の**分数環** (ring of fractions) ということにし，これを $S^{-1}A$ と表す．

明らかに $S^{-1}A$ は可換環となり（なぜならば，$a/s + a'/s' = (s'a + sa')/ss'$，$(a/s) \cdot (a'/s') = aa'/ss'$ と A から自然に可換環の構造が入るから），A を含む（$1 \in S$ であるから）．$S = A \setminus (0)$ ならば，$S^{-1}A = K$ である．S が 1 しか含まないならば，あるいは A の単元しか含まなければ，$S^{-1}A = A$ である．

命題 1. A は整域，S を $A\setminus(0)$ の部分集合で 1 を含み乗法に関して閉じている集合とする．$A'=S^{-1}A$ とおく．

(1) A' の任意のイデアル $\mathfrak{b}'$ に対して，$(\mathfrak{b}'\cap A)A'=\mathfrak{b}'$ であり，よって写像 $\mathfrak{b}'\mapsto\mathfrak{b}'\cap A$ は A' のイデアルの集合から A のイデアルの集合への（包含関係に関して）増大的な単射である．

(2) A' の素イデアルからなる（包含関係に関する）半順序集合から A の素イデアル $\mathfrak{p}$ で $\mathfrak{p}\cap S=\emptyset$ をみたすものからなる半順序集合への写像 $\mathfrak{p}'\mapsto\mathfrak{p}'\cap A$ は同型（すなわち，順序を保つ全単射）である．逆写像は $\mathfrak{p}\mapsto\mathfrak{p}A'$ で与えられる．

証明 (1) $\mathfrak{b}'$ を A' のイデアルとすれば，$\mathfrak{b}'\cap A\subset\mathfrak{b}'$ であり，$\mathfrak{b}'$ がイデアルであるから $(\mathfrak{b}'\cap A)A'\subset\mathfrak{b}'$ である．逆の包含関係を示すために，$x\in\mathfrak{b}'$ をとる．$x=a/s\ (a\in A,s\in S)$ であるから，$sx\in\mathfrak{b}'$ となる（$A\subset A'$ で $\mathfrak{b}'$ は A' のイデアルであるから）．よって $a\in\mathfrak{b}'$，そして $a\in\mathfrak{b}'\cap A$ となる．従って，$x=(1/s)a\in(\mathfrak{b}'\cap A)A'$ となり，$\mathfrak{b}'\subset(\mathfrak{b}'\cap A)A'$，結局 $\mathfrak{b}'=(\mathfrak{b}'\cap A)A'$ を得る．この等式が写像 $\phi:\mathfrak{b}'\mapsto\mathfrak{b}'\cap A$ が単射であることを保証する．なぜなら，写像 $\theta:\mathfrak{b}\mapsto A'\mathfrak{b}$ があって $\theta\cdot\phi=1$ となるからである．ϕ が増大的な写像であることは明らかである．

(2) $\mathfrak{p}'$ を A' の素イデアルとすれば，$\mathfrak{p}=\mathfrak{p}'\cap A$ は A の素イデアルである（3.3 節補題 1）．さらに，$\mathfrak{p}\cap S=\emptyset$ である．なぜならば，もし $s\in\mathfrak{p}\cap S$ とすれば $s\in\mathfrak{p}'$ で $1=(1/s)s\in A'\mathfrak{p}'=\mathfrak{p}'$ となり不合理であるからである．逆に，$\mathfrak{p}$ を A の素イデアルで $\mathfrak{p}\cap S=\emptyset$ とする．$\mathfrak{p}A'$ が A' の素イデアルで $\mathfrak{p}A'\cap A=\mathfrak{p}$ となることを示そう．まず，$\mathfrak{p}A'$ は A' の元で $p/s\ (p\in\mathfrak{p},s\in S)$ の形の元全体の集合である．つまり，任意の元 $x\in\mathfrak{p}A'$ は

$$x=\sum_{i=1}^{n}\frac{a_i}{s_i}p_i \qquad (a_i\in A,s_i\in S,p_i\in\mathfrak{p})$$

の形に書け，

$$x=\sum_{i=1}^{n}\frac{b_i}{s}p_i \qquad \left(s=s_1\cdots s_n,\ \frac{b_i}{s}=\frac{a_i}{s_i}\right)$$

となるので，$x=p/s$ と書けるのである．ここで $p=\sum b_ip_i\in\mathfrak{p}$ である．

$\mathfrak{p} \cap S = \emptyset$ かつ 1 は p/s $(p \in \mathfrak{p}, s \in S)$ の形で書けないから，$1 \notin \mathfrak{p}A'$ という結論を得る．イデアル $\mathfrak{p}A'$ が素イデアルであることを示すため，$a/s \in A'$ と $b/t \in A'$ を $(a/s)\cdot(b/t) \in \mathfrak{p}A'$ となるものとする．このとき，$(a/s)\cdot(b/t) = p/u$ $(p \in \mathfrak{p}, u \in S)$ と書け，$abu = pst \in \mathfrak{p}$ となる．$\mathfrak{p} \cap S = \emptyset$ であるから $u \notin \mathfrak{p}$，よって $ab \in \mathfrak{p}$（$\mathfrak{p}$ は素イデアルであるから）である．これは a または b が $\mathfrak{p}$ に属していることを示している．従って a/s または b/t は $\mathfrak{p}A'$ に属することがわかる．すなわち，$\mathfrak{p}A'$ は素イデアルである．最後に $\mathfrak{p} = \mathfrak{p}A' \cap A$ を示す．明らかに $\mathfrak{p} \subset \mathfrak{p}A' \cap A$ である．逆の包含関係を示すために，$x \in \mathfrak{p}A' \cap A$ をとる．このとき，仮定より $x \in \mathfrak{p}A'$ であるから $x = p/s$ $(p \in \mathfrak{p},\ s \in S)$ と書ける．よって $sx = p \in \mathfrak{p}$ となる．$s \notin \mathfrak{p}$ $(\mathfrak{p} \cap S = \emptyset)$ で $\mathfrak{p}$ は素イデアルであることから，$x \in \mathfrak{p}$ となる．さて，$\mathfrak{p} = \mathfrak{p}A' \cap A$ と $\mathfrak{p}' = A'(\mathfrak{p}' \cap A)$ であることより，写像 $\phi : \mathfrak{p}' \mapsto \mathfrak{p}' \cap A$ と $\theta : \mathfrak{p} \mapsto \mathfrak{p}A'$（素イデアル $\mathfrak{p}$ は S と共通部分をもたないものに限る）は，$\phi\cdot\theta$ と $\theta\cdot\phi$ がともに恒等写像となるから，逆の全単射であることが容易にわかる． □

系. A が Noether 整域ならば，すべての分数環 $S^{-1}A$ は Noether 環である．

証明 命題 1(1) より，$S^{-1}A$ のイデアルの順序集合から A のイデアルの順序集合の部分順序集合への単射が存在する．従って $S^{-1}A$ のイデアルの順序集合は極大条件をみたし，$S^{-1}A$ が Noether 環ということがいえる． □

命題 2. R を整域，A を R の部分環，S を乗法に関して閉じている A の部分集合で $1 \in S, 0 \notin S$ とする．B を A の R における整閉包とする．このとき，$S^{-1}A$ の $S^{-1}R$ における整閉包は $S^{-1}B$ である．

証明 $S^{-1}B$ の任意の元は b/s $(b \in B, s \in S)$ の形に表せる．b の A 上の整従属方程式

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0 \qquad (a_i \in A)$$

を s^n で割ることにより

$$\left(\frac{b}{s}\right)^n + \frac{a_{n-1}}{s}\left(\frac{b}{s}\right)^{n-1} + \cdots + \frac{a_0}{s^n} = 0$$

を得る．これは b/s が $S^{-1}A$ 上整であることを示している．逆に $S^{-1}R$ の元 x/s $(x \in R, s \in S)$ が $S^{-1}A$ 上整であるとすれば，次のような方程式

$$\left(\frac{x}{s}\right)^n + \frac{a_{n-1}}{t_{n-1}}\left(\frac{x}{s}\right)^{n-1} + \cdots + \frac{a_0}{t_0} = 0 \quad (a_i \in A, t_i \in S)$$

が存在する．$(t_0t_1\cdots t_{n-1})^n$ を両辺に掛けることによって，$xt_0\cdots t_{n-1}/s$ が A 上整であることがわかる．よって $xt_0\cdots t_{n-1}/s \in B$ となり，$x/s = (1/t_0\cdots t_{n-1})(xt_0\cdots t_{n-1}/s)$ は $S^{-1}B$ に属する． □

系． A が整閉環ならば，任意の分数環 $S^{-1}A$ は整閉である．

証明　命題 2 において R として A の分数体をとればよい． □

命題 3． A が Dedekind 環ならば，任意の分数環 $S^{-1}A$ は Dedekind 環である．

証明　$S^{-1}A$ は Noether 環（命題 1 の系）であり，整閉である（命題 2 の系）．さらに，A から $S^{-1}A$ に移ることによっていくつかの素イデアルを「失う」（命題 1(2)）だけであるから，$S^{-1}A$ の (0) でない任意の素イデアルは極大である． □

命題 4． A を Dedekind 環，$\mathfrak{p}$ を A の (0) でない素イデアル，$S = A \setminus \mathfrak{p}$ とする．このとき $S^{-1}A$ は単項イデアル環である．より正確には，ある素元 $p \in S^{-1}A$ が存在して，$S^{-1}A$ の (0) でないイデアルは $(p^n), n \geq 0$ の形となるものだけである．

証明　$\mathfrak{p}$ は S と共通部分をもたない A の (0) でない唯 1 つの素イデアルであるから，$S^{-1}A$ の (0) でない素イデアルは $\mathfrak{P} = \mathfrak{p}S^{-1}A$ のみである（命題 1, 2）．$S^{-1}A$ は Dedekind 環である（命題 3）から，その (0) でないイデアルは $\mathfrak{P}^n$ $(n \geq 0)$ の形のものだけである．$p \in \mathfrak{P} \setminus \mathfrak{P}^2$ をとると，イデアル (p) は $\mathfrak{P}$ に含まれ，$\mathfrak{P}^2$ には含まれない．従って，$(p) = \mathfrak{P}$ であり，任意の $n \geq 0$ に対して $(p^n) = \mathfrak{P}^n$ となる．よって $S^{-1}A$ は単項イデアル環であり，そのイデアルはすべて $(p^n), n \geq 0$ の形である． □

命題 5. A を整域，S を乗法に関して閉じていて 1 を含む $A \setminus (0)$ の部分集合，$\mathfrak{m}$ を A の極大イデアルで S と共通部分をもたないものとする．このとき，

$$S^{-1}A/\mathfrak{m}S^{-1}A \cong A/\mathfrak{m}$$

である．

証明 環の準同型の合成 $A \to S^{-1}A \to S^{-1}A/\mathfrak{m}S^{-1}A$ は核 $\mathfrak{m}S^{-1}A \cap A = \mathfrak{m}$ をもつ．よって単射 $\phi : A/\mathfrak{m} \to S^{-1}A/\mathfrak{m}S^{-1}A$ がひき起こされる．次に ϕ が全射であることを示す．$x = a/s \in S^{-1}A$ $(a \in A, s \in S)$ をとり，$\overline{x}$ を $S^{-1}A/\mathfrak{m}S^{-1}A$ における x の剰余類とする．$s \notin \mathfrak{m}$（仮定 $\mathfrak{m} \cap S = \emptyset$ より）と，$\mathfrak{m}$ が極大であることより，$b \in A$ が存在して $bs \equiv 1 \pmod{\mathfrak{m}}$ となる．よって

$$\frac{a}{s} - ab = \frac{a}{s}(1 - bs) \in \mathfrak{m}S^{-1}A.$$

これより，$\phi(ab) = \overline{x}$ となる． □

5.2 拡大における素イデアルの分解

この節においては，A は標数 0 の Dedekind 環，K をその分数体，L を K の n 次の有限拡大，B を A の L における整閉包とする．B は Dedekind 環であった（3.4 節定理 1）．

$\mathfrak{p}$ を A の (0) でない素イデアルとする．このとき，$\mathfrak{p}B$ は B のイデアルで，それは

$$\mathfrak{p}B = \prod_{i=1}^{q} \mathfrak{P}_i^{e_i} \tag{1}$$

の形で表される．ここで，$\mathfrak{P}_i$ は B の相異なる素イデアルで，e_i は正の整数，積の記号はイデアルの積を表すものとする．

命題 1. $\mathfrak{P}_i$ の全体の集合は B の素イデアル $\mathfrak{Q}$ で $\mathfrak{Q} \cap A = \mathfrak{p}$ となるもの全体の集合と一致する．

証明 B の素イデアル $\mathfrak{Q}$ について，$\mathfrak{Q} \cap A = \mathfrak{p}$ であることは $\mathfrak{Q} \supset \mathfrak{p}B$ であ

ることと同値である（⇒ は明らか．⇐ は $\mathfrak{Q}\cap A$ が A の素イデアルで $\mathfrak{p}$ が極大であることによる）．明らかに，$\mathfrak{p}B=\prod_{i=1}^{q}\mathfrak{P}_i^{e_i}$ は各 $i=1,\dots,q$ に対して $\mathfrak{p}B\subset\mathfrak{P}_i$ が成り立つことを示している．よって $\mathfrak{P}_i$ が $\mathfrak{p}B$ の積の形の中に現れることは $\mathfrak{P}_i\cap A=\mathfrak{p}$ であることが必要十分である．　□

さて，$A/\mathfrak{p}$ は各 $i=1,\dots,q$ について $B/\mathfrak{P}_i$ の部分環として同一視してよい．どちらの環も体である．B は有限型の A-加群（3.4 節定理 1）であるから，$B/\mathfrak{P}_i$ は $A/\mathfrak{p}$ 上の有限次元のベクトル空間である．f_i で $B/\mathfrak{P}_i$ の $A/\mathfrak{p}$ 上の次元を表すことにし，f_i を $\mathfrak{P}_i$ の A 上の**剰余次数** (residual degree) とよぶことにする．(1) における指数 e_i を $\mathfrak{P}_i$ の A 上の**分岐指数** (ramification index) という．最後に，$\mathfrak{p}B\cap A=\mathfrak{p}$（⊃ は明らか．⊂ は各 $i=1,\dots,q$ について $\mathfrak{P}_i\cap A=\mathfrak{p}$ であることによる）が成り立つので，$B/\mathfrak{p}B$ は $A/\mathfrak{p}$ 上のベクトル空間であり，有限次元であることに注意しよう．

定理 1. 上の記号の下で，

$$\sum_{i=1}^{q}e_if_i=[B/\mathfrak{p}B:A/\mathfrak{p}]=n \tag{2}$$

が成り立つ．

証明　第 1 の等号は容易である．イデアルの列

$$B\supset\mathfrak{P}_1\supset\mathfrak{P}_1^2\supset\cdots\supset\mathfrak{P}_1^{e_1}\supset\mathfrak{P}_1^{e_1}\mathfrak{P}_2\supset\cdots\supset\mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\supset\cdots\supset\mathfrak{P}_1^{e_1}\cdots\mathfrak{P}_q^{e_q}=\mathfrak{p}B$$

を考える．この列の連続した 2 つの項は $\mathfrak{B}$ と $\mathfrak{B}\mathfrak{P}_i$ という形になっている．$\mathfrak{B}$ と $\mathfrak{B}\mathfrak{P}_i$ の間にはまったくイデアルはないから，$\mathfrak{B}/\mathfrak{B}\mathfrak{P}_i$ は $B/\mathfrak{P}_i$ 上のベクトル空間として 1 次元である（3.5 節命題の証明を参照）．よって，$\mathfrak{B}/\mathfrak{B}\mathfrak{P}_i$ は $A/\mathfrak{p}$ 上の f_i 次元のベクトル空間である．上の列において，与えられた i に対し，$\mathfrak{B}/\mathfrak{B}\mathfrak{P}_i$（すなわち $A/\mathfrak{p}$ 上の次元が f_i である）の形をした剰余空間を結びつけるような連続した項はちょうど e_i 個である．全体の次元 $[B/\mathfrak{p}B:A/\mathfrak{p}]$ は各剰余空間の次元の和であるから，それは $\sum_{i=1}^{q}e_if_i$ に等しい．

第 2 の等号も B が自由 A-加群のときは容易である．特に A が単項イデアル環ならば簡単である（2.7 節定理 1 の系）．この場合，B の A-加群としての基底 $\{x_1,\dots,x_n\}$ は mod $\mathfrak{p}B$ で考えて，$B/\mathfrak{p}B$ の $A/\mathfrak{p}$ 上の基底とな

る．A の乗法に関して閉じている部分集合 $S = A \setminus \mathfrak{p}$，分数環 $A' = S^{-1}A$ と $B' = S^{-1}B$ を考えることにより，一般の場合を上記の場合に帰着することにしよう．A' は $\mathfrak{p}A'$ を唯 1 つの極大イデアルとしてもつ単項イデアル環であり（5.1 節命題 4），B' は A' の L における整閉包である（5.1 節命題 2）ことはわかっている．A が単項イデアル環である特殊な場合によって，$[B'/\mathfrak{p}B' : A'/\mathfrak{p}A'] = n$ となる．さて Dedekind 環 B' のイデアル $\mathfrak{p}B'$ の分解を考えよう．$\mathfrak{p}B = \prod_{i=1}^{q} \mathfrak{P}_i^{e_i}$ であることより，$\mathfrak{p}B' = \prod_{i=1}^{q}(\mathfrak{P}_i B')^{e_i}$ を得る．$\mathfrak{P}_i \cap A = \mathfrak{p}$（命題 1）であるから，$\mathfrak{P}_i \cap S = \emptyset$ で $\mathfrak{P}_i B'$ は B' の (0) でない素イデアルである（5.1 節命題 1(2)）．証明の第 1 の部分より，

$$[B'/\mathfrak{p}B' : A'/\mathfrak{p}A'] = \sum_{i=1}^{q} e_i [B'/\mathfrak{P}_i B' : A'/\mathfrak{p}A']$$

を得る．ところで，5.1 節命題 5 より

$$A'/\mathfrak{p}A' \cong A/\mathfrak{p}, \quad B'/\mathfrak{P}_i B' \cong B/\mathfrak{P}_i$$

である．従って

$$n = [B'/\mathfrak{p}B' : A'/\mathfrak{p}A'] = \sum_{i=1}^{q} e_i f_i$$

となる． □

命題 2. 上と同じ記号の下で，環 $B/\mathfrak{p}B$ は環 $\prod_{i=1}^{q} B/\mathfrak{P}_i^{e_i}$ と同型である．

証明 $\mathfrak{P}_i$ は $\mathfrak{P}_i^{e_i}$ を含む B の唯 1 つの極大イデアルである．よって $\mathfrak{P}_i^{e_i} + \mathfrak{P}_j^{e_j} = B$ $(i \neq j)$ である．この命題は等式 (1) と 1.3 節の補題 1 により得られる． □

円分体の例. p を素数，z を $\mathbb{C}$ における 1 の原始 p^r-乗根とする．この場合，複素数の 1 の p^r-乗根のすべては z^j $(j = 1, \ldots, p^r)$ の形である．1 の原始 p^r-乗根は j が p の倍数でないものである．原始 p^r-乗根の個数は

$$\varphi(p^r) = p^r - p^{r-1} = p^{r-1}(p-1)$$

である（1.6 節を参照）．1 の原始 p^r-乗根は円分多項式

$$F(X) = \frac{X^{p^r} - 1}{X^{p^{r-1}} - 1} = X^{p^{r-1}(p-1)} + X^{p^{r-1}(p-2)} + \cdots + X^{p^{r-1}} + 1 \quad (3)$$

の根と等しい．

ここで，$[\mathbb{Q}[z]:\mathbb{Q}]=p^{r-1}(p-1)$，すなわち $F(X)$ は既約である（2.9 節を参照）ことの別証明を与えることにする．このために，$e=p^{r-1}(p-1)$ とおき，$z_1,\ldots,z_e$ を 1 の原始 p^r-乗根の全体とする．$F(X+1)$ の定数項は p であることより，

$$\prod_{j=1}^{e}(z_j-1)=\pm p$$

がでる．B を $\mathbb{Q}[z]$ の整数環とする．明らかに任意の j,k に対して $z_j\in B$ で $z_j-1\in(z_k-1)B$ となる．なぜならば z_j は z_k のべき z_k^q であり，$z_k^q-1=(z_k-1)(z_k^{q-1}+\cdots+z_k+1)$ であるからである．よってすべてのイデアル $(z_k-1)B$ は同一である．従って $pB=(z_1-1)^eB$ を得る．

さて，$pB=\prod_{i=1}^{q}\mathfrak{P}_i^{e_i}$ と表す．ここで $\mathfrak{P}_i$ は B の素イデアルである．各 e_i が e の倍数であることは明らかである．ところで $e\geq[\mathbb{Q}[z]:\mathbb{Q}]$ である（(3) より）ので，$e\geq\sum_{i=1}^{q}e_if_i$（定理 1）である．これらの不等式（実は等式）より，$q=1, e=e_1, f_1=1$ で $[\mathbb{Q}[z]:\mathbb{Q}]=e$ であることが結論される．まとめると次のようになる，すなわち

(a) $[\mathbb{Q}[z]:\mathbb{Q}]=e=p^{r-1}(p-1)$,

(b) $(z_1-1)B$ は剰余次数 1 の B の素イデアルである，

(c) $pB=(z_1-1)^eB$.

5.3　判別式と分岐

5.2 節の記号を用いて（$\mathfrak{p}B=\prod_{i=1}^{q}\mathfrak{P}_i^{e_i}$ とする），A の素イデアル $\mathfrak{p}$ は分岐指数 e_i のどれかが 1 つでも 1 より大きいとき，B（あるいは，L）において**分岐する** (ramify) といわれる．判別式（2.7 節）の理論のことばを用いて，B において分岐する A の素イデアルを特徴づけることにしよう．特に，B において分岐する A の素イデアルは高々有限個であることを示す．まず，判別式についてのいくつかの補題が必要である．

補題 1. A を環，$B_1,\ldots,B_q$ を A を含む環で，有限型の自由 A-加群である

とする．$B=\prod_{i=1}^{q} B_i$ を環の直積とする．このとき，

$$\mathfrak{D}_{B/A}=\prod_{i=1}^{q}\mathfrak{D}_{B_i/A}$$

(2.7 節定義 2 を参照) である．

証明 $q=2$ のときを証明する．一般の場合は q についての帰納法による．$\{x_1,\ldots,x_m\}$ と $\{y_1,\ldots,y_n\}$ をそれぞれ B_1 と B_2 の A 上の加群としての基底とする．いつものように，B_1 と $B_1\times(0)$，B_2 と $(0)\times B_2$ を同一視すると，$\{x_1,\ldots,x_m,y_1,\ldots,y_n\}$ は $B=B_1\times B_2$ の A 上の基底と考えられる．環の直積の定義により $x_iy_j=0$ であり，これより $\mathrm{Tr}(x_iy_j)=0$ となる．その結果，行列式 $D(x_1,\ldots,x_m,y_1,\ldots,y_n)$ は次の行列の行列式である．

$$\left[\begin{array}{c:c} \mathrm{Tr}(x_ix_{i'}) & O \\ \hdashline O & \mathrm{Tr}(y_jy_{j'}) \end{array}\right].$$

この行列式の値は $\det(\mathrm{Tr}(x_ix_{i'}))\cdot\det(\mathrm{Tr}(y_jy_{j'}))$ に等しいから，

$$D(x_1,\ldots,x_m,y_1,\ldots,y_n)=D(x_1,\ldots,x_m)D(y_1,\ldots,y_m)$$

となる． □

補題 2. B を環，A を B の部分環，$\mathfrak{a}$ を A のイデアルとする．B が A 上の自由加群でその基底を $\{x_1,\ldots,x_n\}$ とする．$x\in B$ について $\overline{x}$ で $B/\mathfrak{a}B$ における剰余類を表す．このとき，$\{\overline{x_1},\ldots,\overline{x_n}\}$ は $B/\mathfrak{a}B$ の $A/\mathfrak{a}$ 上の基底であり，

$$D(\overline{x_1},\ldots,\overline{x_n})=\overline{D(x_1,\ldots,x_n)} \tag{1}$$

である．

証明 $x\in B$ とする．x を掛けるという変換に対しての基底 $\{x_1,\ldots,x_n\}$ に関する行列を $(a_{ij})\quad(a_{ij}\in A)$ とすれば，$\overline{x}$ を掛けるという変換に対しての基底 $\{\overline{x_1},\ldots,\overline{x_n}\}$ に関する行列は $(\overline{a_{ij}})$ である．よって $\mathrm{Tr}(\overline{x})=\overline{\mathrm{Tr}(x)}$ である．x として x_ix_j を考えれば $\mathrm{Tr}(\overline{x_i}\cdot\overline{x_j})=\overline{\mathrm{Tr}(x_ix_j)}$ であり，(1) は行列式をとることにより得られる． □

補題 3. K を有限体もしくは標数 0 の体とする．L を有限次元の（可換）K-代数とする．このとき L が被約 (reduced) であるためには $\mathfrak{D}_{L/K} \neq (0)$ が必要十分である．

証明　まず，L が被約でないと仮定して，x が L の 0 でないべき零元とする．$\{x_1, \ldots, x_n\}$ を L の K 上の基底で $x = x_1$ とする．このとき，$x_1 x_j$ はべき零で，$x_1 x_j$ を掛けることは K 上のベクトル空間 L のべき零な自己準同型である．よってこの自己準同型のすべての固有値は 0 であり，$\mathrm{Tr}(x_1 x_j) = 0$ となる．行列 $(\mathrm{Tr}(x_i x_j))$ は成分が 0 だけからなる行をもち，これは $D(x_1, \ldots, x_n) = 0$，すなわち $\mathfrak{D}_{L/K} = (0)$ を示している．

逆に，L は被約であると仮定する．このとき L のイデアル (0) は有限個の素イデアルの共通部分で表される，すなわち $(0) = \bigcap_{i=1}^{q} \mathfrak{P}_i$（4.7 節補題）である．$L/\mathfrak{P}_i$ は整域で，K 上有限次元の代数であるから，体である（2.1 節命題 3）．よって $\mathfrak{P}_i$ は L の極大イデアルであり，結局，$\mathfrak{P}_i + \mathfrak{P}_j = L \quad (i \neq j)$ が成り立つ．従って，L は直積環 $\prod_{i=1}^{q} L/\mathfrak{P}_i$ と同型になる（1.3 節補題 1）．補題 1 より，$\mathfrak{D}_{L/K} = \prod \mathfrak{D}_{(L/\mathfrak{P}_i)/K}$ である．ところで K は有限体または標数 0 の体であったから $\mathfrak{D}_{(L/\mathfrak{P}_i)/K} \neq (0)$ である（2.7 節命題 3）．従って $\mathfrak{D}_{L/K} \neq (0)$ である．　□

定義 1. K, L は数体で $K \subset L$ とする．A と B をそれぞれ K と L の整数環とする．L の K 上の基底で B に含まれるものの判別式のすべてによって生成された A のイデアルを B の A 上の（または L の K 上の）**判別式**（イデアル）とよび，これを $\mathfrak{D}_{B/A}$ または $\mathfrak{D}_{L/K}$ と表す．

注意 1. $\{x_1, \ldots, x_n\}$ が L の K 上の基底で B に含まれているとすると，$\mathrm{Tr}_{L/K}(x_i x_j) \in A$（2.6 節命題 2 の系），従って $D(x_1, \ldots, x_n) \in A$ となる．よって $\mathfrak{D}_{B/A}$ は A の整イデアルである．2.7 節命題 3 より，これは (0) ではない．

注意 2. B が自由 A-加群（たとえば，A が単項イデアル環）のとき，判別式 $\mathfrak{D}_{B/A}$ は $D(e_1, \ldots, e_n)$ によって生成されたイデアルとして定義されていた（2.7 節定義 2）．ここで $\{e_1, \ldots, e_n\}$ は B の A-加群としての基底で

ある．以前に定義されたものは上記で与えられたものと一致する．なぜならば，L の K 上の任意の基底 $\{x_i\} \subset B$ が与えられたとき，$x_i = \sum_j a_{ij}e_j$ $(a_{ij} \in A)$ と表せ，

$$D(x_1, \ldots, x_n) = \det(a_{ij})^2 D(e_1, \ldots, e_n)$$

（2.7 節命題 1）となるからである．

定理 1． 記号は定義 1 におけるものと同じとする．A の素イデアル $\mathfrak{p}$ が B において分岐するための必要十分条件は $\mathfrak{p}$ が判別式 $\mathfrak{D}_{B/A}$ を含むことである．従って，B において分岐する A の素イデアルは高々有限個である．

証明 $\mathfrak{D}_{B/A} \neq (0)$ であることを考えれば第 2 の主張は第 1 の主張から出る．第 1 の主張を証明しよう．$B/\mathfrak{p}B \cong \prod_{i=1}^{q} B/\mathfrak{P}_i^{e_i}$（5.2 節命題 2）であるから，「$\mathfrak{p}$ が分岐する」ということは「$B/\mathfrak{p}B$ が被約でない」ということ，すなわち，「$\mathfrak{D}_{(B/\mathfrak{p}B)/(A/\mathfrak{p})} = (0)$」ということと同値である（補題 3 と $A/\mathfrak{p}$ が有限体であることによる）．さて，$S = A \setminus \mathfrak{p}$, $A' = S^{-1}A$, $B' = S^{-1}B$, $\mathfrak{p}' = \mathfrak{p}A'$ とおく．このとき A' は単項イデアル環（5.1 節命題 4），B' は自由 A'-加群，$A/\mathfrak{p} \cong A'/\mathfrak{p}'$, $B/\mathfrak{p}B \cong B'/\mathfrak{p}'B'$ である（5.1 節命題 5）．従って，B' の A'-加群としての基底を $\{e_1, \ldots, e_n\}$ と表すと，$\mathfrak{D}_{(B/\mathfrak{p}B)/(A/\mathfrak{p})} = (0)$ であることは $D(e_1, \ldots, e_n) \in \mathfrak{p}'$ であることと同値である（補題 2）．$D(e_1, \ldots, e_n) \in \mathfrak{p}'$ で，$\{x_1, \ldots, x_n\}$ が L の K 上の基底で B に含まれているとすれば，$x_i = \sum a'_{ij}e_j$, $a_{ij} \in A'$ と書ける（$B \subset B'$ であるから）ので，

$$D(x_1, \ldots, x_n) = \det(a'_{ij})^2 D(e_1, \ldots, e_n) \in \mathfrak{p}'$$

となる．$\mathfrak{p}' \cap A = \mathfrak{p}$（5.1 節命題 1(2)）であるから，$D(x_1, \ldots, x_n) \in \mathfrak{p}$，そして $\mathfrak{D}_{B/A} \subset \mathfrak{p}$ と結論できる．逆に，$\mathfrak{D}_{B/A} \subset \mathfrak{p}$ とすれば，$D(e_1, \ldots, e_n) \in \mathfrak{p}'$ である．というのは，$e_i = y_i s^{-1}$ $(y_i \in B,\ s \in S,\ 1 \leq i \leq n)$ と書けるからである．従って

$$D(e_1, \ldots, e_n) = s^{-2n} D(y_1, \ldots, y_n) \in \mathfrak{D}_{B/A}A' \subset \mathfrak{p}A' = \mathfrak{p}'$$

となる．□

例 1（2 次体）． $K = \mathbb{Q}, L = \mathbb{Q}[d]$，$d$ は平方因子をもたない整数，とする

(2.5 節)．

(a)　$d \equiv 2$ または 3 (mod 4) のとき，$\{1, \sqrt{d}\}$ が L の整数環の基底である．$\mathrm{Tr}(1) = 2$, $\mathrm{Tr}(\sqrt{d}) = 0$, $\mathrm{Tr}(d) = 2d$ であるから，$D(1, \sqrt{d}) = 4d$ となる．従って L において分岐する素数は 2 と d の素因数を含む．

(b)　$d \equiv 1$ (mod 4) のとき，$\{1, (1+\sqrt{d})/2\}$ が L の整数環の基底である．ここで，

$$\mathrm{Tr}(1) = 2, \quad \mathrm{Tr}\left(\frac{1+\sqrt{d}}{2}\right) = 1,$$

$$\mathrm{Tr}\left(\left(\frac{1+\sqrt{d}}{2}\right)^2\right) = \mathrm{Tr}\left(\frac{1+d}{4} + \frac{1}{2}\sqrt{d}\right) = \frac{d+1}{2}$$

がわかり，よって

$$D\left(1, \frac{1+\sqrt{d}}{2}\right) = 2 \cdot \frac{d+1}{2} - 1 = d$$

となる．L において分岐する素数は d の素因数のみである．

2 次体 $\mathbb{Q}[\sqrt{d}]$ はその判別式 D によって一意的に決定される．実際，

$D \equiv 0$ (mod 4) ならば $d = \frac{D}{4}$ （必然的に $d \equiv 2$ または 3 (mod 4)），

$D \equiv 1$ (mod 4) ならば $d = D$,

$D \equiv 2$ または 3 (mod 4) はありえない．

例 2（円分体）．p を奇素数，z を複素数の 1 の原始 p 乗根，$L = \mathbb{Q}[z]$ を対応する円分体とする．このとき $\{1, z, \ldots, z^{p-2}\}$ は L の整数環 B の $\mathbb{Z}$-基底であり（2.9 節定理 2），z の $\mathbb{Q}$ 上の最小多項式 $F(X)$ は $(X-1)F(X) = X^p - 1$ の関係をみたす（同上，定理 1）ことはわかっている．次の等式を用いて，判別式 $\mathfrak{D}_{B/\mathbb{Z}}$ を計算してみよう．2.7 節 (6) より

$$D(1, z, \ldots, z^{p-2}) = (-1)^{\frac{1}{2}(p-1)(p-2)} \mathrm{N}(F'(z))$$

である．$(X-1)F(X) = X^p - 1$ の両辺の導関数を考えると，$(z-1)F'(z) = pz^{p-1}$ を得る（$F(z) = 0$ だから）．$\mathrm{N}(p) = p^{p-1}, \mathrm{N}(z) = \pm 1, \mathrm{N}(z-1) = \pm p$

がわかっている（2.9 節）ので，

$$D(1, z, \ldots, z^{p-2}) = \pm p^{p-2}. \tag{1}$$

これより，p は $\mathbb{Q}[z]$ において分岐する唯 1 つの素数であることがわかる．

次の結果は，数体の整数環を決定するのにしばしば役に立つ．

命題 1. L を $\mathbb{Q}$ 上の n 次の数体，$\{x_1, \ldots, x_n\}$ を L の整数環 B に含まれる L の $\mathbb{Q}$-基底とする．判別式 $D(x_1, \ldots, x_n)$ が平方因子をもたないならば，$\{x_1, \ldots, x_n\}$ は B の $\mathbb{Z}$-基底である．

証明 $\{e_1, \ldots, e_n\}$ を B の $\mathbb{Z}$-基底とすると，$x_i = \sum_{j=1}^{n} a_{ij} e_j$，$a_{ij} \in \mathbb{Z}$ と書け，

$$D(x_1, \ldots, x_n) = \det(a_{ij})^2 D(e_1, \ldots, e_n)$$

を得る．$D(x_1, \ldots, x_n)$ は平方因子をもたないので，$\det(a_{ij})$ は ± 1 でなければならない．よって $\{x_1, \ldots, x_n\}$ も B の $\mathbb{Z}$-基底である． □

∞ 円分体 $(p \geq 5)$ または 2 次体は命題 1 の十分条件が必要条件ではないという例を与える．

例. 多項式 $X^3 - X - 1$（あるいは，$X^3 + X + 1, X^3 + 10X + 1$）は $\mathbb{Q}$ 上既約である（実際，そうでないとすると，1 次の因数をもってしまう，すなわち，有理数解 $x \in \mathbb{Q}$ をもってしまう．しかしこの多項式は最高次の係数が 1 であるから，$x \in \mathbb{Q}$ は $x \in \mathbb{Z}$ を意味する．この多項式の定数項は 1 であるから，$x = \pm 1$ である（x は定数項を割り切らなければならない）．± 1 のどちらもこの多項式をみたさないことを確認すれば，この多項式が既約であることがわかる）．

さて，x を与えられた多項式の複素数解とする．体 $L = \mathbb{Q}[x]$ は 3 次体（すなわち，次数 3）である．よって $\{1, x, x^2\}$ は L の $\mathbb{Q}$ 上の基底であり，明らかに x は L の整数である．2.7 節 (7) より，$D(1, x, x^2) = 4 - 27 = -23$（あるいは $-31, -4027$）であり，これは素数を負にしたものである．従って $\{1, x, x^2\}$ は L の整数環の $\mathbb{Z}$-基底である．

5.4　2次体における素数の分解

$d \in \mathbb{Z}$ は平方因子をもたない整数，L は2次体 $\mathbb{Q}[d]$，B は L の整数環，p は素数とする．イデアル pB を B の素イデアルの積に分解することを考えよう．

公式 $\sum_{i=1}^{q} e_i f_i = 2$（5.2節定理1）より $q \leq 2$ がわかり，次の3つの可能性がある，すなわち，

(a) $q = 2,\ \ e_1 = e_2 = 1,\ \ f_1 = f_2 = 1.$
　この場合，p は L で**分解する**という．

(b) $q = 1,\ \ e_1 = 1,\ \ f_1 = 2.$
　この場合は，p は L で**素を保つ**という．

(c) $q = 1,\ \ e_1 = 2,\ \ f_1 = 1.$
　この場合は，p は L で**分岐する**という．

まず，p が奇素数の場合を考える．d の値に従って $B = \mathbb{Z} + \sqrt{d}\mathbb{Z}$ または $B = \mathbb{Z} + \frac{1}{2}(1+\sqrt{d})\mathbb{Z}$ となることがわかっている（2.5節）．ところで，もし B から pB を法とした剰余類に移ると，第2の場合は，$a + b(\frac{1}{2}(1+\sqrt{d}))$（$b$ は奇数）が $a + (b+p)(\frac{1}{2}(1+\sqrt{d}))$ に合同であり，$\mathbb{Z} + \sqrt{d}\mathbb{Z}$ に属することがわかる．よって任意の d に対して，$B/pB \cong (\mathbb{Z} + \sqrt{d}\mathbb{Z})/(p)$ を得る．また，$\mathbb{Z} + \sqrt{d}\mathbb{Z} \cong \mathbb{Z}[X]/(X^2 - d)$ であることより，

$$B/pB \cong \mathbb{Z}[X]/(p, X^2 - d) \cong (\mathbb{Z}[X]/(p))/(X^2 - \overline{d}) \cong \mathbb{F}_p[X]/(X^2 - \overline{d}).$$

ここで $\overline{d}$ は d の p を法とした剰余類を表す．さて，p が B で分解（あるいは，素を保つ，分岐する）ということは，次の解釈をもつ．すなわち，B/pB は2つの体の積（あるいは，体，べき零を含む）である（5.2節命題2を参照）．言い換えると，多項式 $X^2 - \overline{d} \in \mathbb{F}_p[X]$ は2つの異なる1次式の積（あるいは，既約，平方）である．これは，$\overline{d}$ が $\mathbb{F}_p$ において0でない平方となる（あるいは，$\mathbb{F}_p$ において平方でない，$\mathbb{F}_p$ において0でない）ときに起きる．$\overline{d}$ が $\mathbb{F}_p$ において0でない平方となる（あるいは，$\mathbb{F}_p$ において平方でない）とき，d は p を法として**平方剰余** (quadratic residue)（あるいは，**平方非剰余** (quadratic non-residue)）であるという．

さて，$p=2$ の場合を考える．$d\equiv 2$ または $3 \pmod 4$ ならば，$B=\mathbb{Z}+\sqrt{d}\mathbb{Z}$ で，上で見たように，$B/2B\cong\mathbb{F}_2[X]/(X^2-\overline{d})$ である．この場合，$X^2-\overline{d}$ は X^2 または $X^2+1=(X+1)^2$ に等しい．どちらの場合も平方なので，よって 2 は B において分岐する．$d\equiv 1 \pmod 4$ ならば，$\frac{1}{2}(1+\sqrt{d})$ は $X^2-X-(d-1)/4$ を最小多項式としてもつ．よって，上で見たように，$B/2B\cong\mathbb{F}_2[X]/(X^2-X-\delta)$ である．ここで δ は $\frac{1}{4}(d-1)$ の 2 を法とした剰余類を表す．$d\equiv 1 \pmod 8$ に対しては，$\delta=0$ であり，$X^2-X-\delta=X(X-1)$ となる．よって 2 は分解する．$d\equiv 5 \pmod 8$ に対しては，$\delta=1$ であり，$X^2-X-\delta=X^2+X+1$ となり，$\mathbb{F}_2[X]$ で既約である．よって 2 は素を保つ．

まとめると，次のことが証明されたことになる．

命題 1. $L=\mathbb{Q}[\sqrt{d}]$ を 2 次体で d は平方因子をもたないとする．

(a) 奇素数 p で，d が法 p で平方剰余であるものは，L で分解する．
$d\equiv 1 \pmod 8$ ならば，2 もそうである．

(b) 奇素数 p で，法 p で d が平方剰余でないものは L で素を保つ．
$d\equiv 5 \pmod 8$ ならば，2 もそうである．

(c) 奇素数 p で d の因子であるものは L で分岐する．
$d\equiv 2$ または $3 \pmod 4$ ならば，2 もそうである．

(c) の部分は以前に 5.3 節において例として証明済みである．

5.5　平方剰余の相互法則

奇素数 p と，p と互いに素な整数 d に対して，5.4 節で導入した言葉，「d は法 p で平方剰余である」（あるいは，「d は法 p で平方非剰余である」）とは $\mathbb{F}_p^*$ において d の法 p での剰余類が平方である（あるいは，平方でない）ということである．そこで，**Legendre 記号** (Legendre symbol)$\left(\frac{d}{p}\right)$ を次のように定義する．

$$\begin{cases} \left(\dfrac{d}{p}\right) = +1 & (d \text{ が法 } p \text{ で平方剰余のとき}) \\ \left(\dfrac{d}{p}\right) = -1 & (d \text{ が法 } p \text{ で平方剰余でないとき}). \end{cases} \tag{1}$$

$\left(\frac{d}{p}\right)$ は整数 d が p と互いに素であるときのみ，すなわち $d \in \mathbb{Z} \setminus p\mathbb{Z}$ のときのみ定義される．乗法群 $\mathbb{F}_p^*$ は偶数 $p-1$ を位数とする巡回群である（1.7 節定理 1）から，$\mathbb{F}_p^*$ における平方は指数 2 の部分群 $(\mathbb{F}_p^*)^2$ をなし，$\mathbb{F}_p^*/(\mathbb{F}_p^*)^2$ は $\{+1,-1\}$ と同型である．明らかに，Legendre 記号は次の準同型の合成である．

$$\mathbb{Z} \setminus p\mathbb{Z} \to \mathbb{F}_p^* \to \mathbb{F}_p^*/(\mathbb{F}_p^*)^2 \simeq \{+1,-1\}.$$

結果として，次の積の公式が出る．

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right), \quad a, b \in \mathbb{Z} \setminus p\mathbb{Z}. \tag{2}$$

命題 1（Euler の判定法）． p が奇素数で，$a \in \mathbb{Z} \setminus p\mathbb{Z}$ ならば，

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

証明　w で法 p での原始根を表す（1.7 節）．このとき，w の剰余類 $\overline{w}$ は $\mathbb{F}_p^*$ を生成するから $a \equiv w^j \pmod{p}$，$0 \le j \le p-2$，と書ける．明らかに，a が平方剰余であるためには j が偶数であることが必要十分である．従って $\left(\frac{a}{p}\right) = (-1)^j$ である．他方，$\mathbb{F}_p^*$ は位数 2 の元を唯 1 つしかもたない．この元は $\overline{w}^{\frac{p-1}{2}}$ で，平方が 1 であるから -1 に等しい．$\mathbb{Z}$ において，$-1 \equiv w^{\frac{p-1}{2}} \pmod{p}$ である．よって

$$\left(\frac{a}{p}\right) = (-1)^j \equiv w^{j \cdot \frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

□

さて，有名な定理を証明しよう．それは，異なる奇素数を法とする合同の性質が互いに無関係でないことを示している．

定理 1（Legendre-Gauss の平方剰余の相互法則）． p と q が異なる奇素数とすれば

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

証明　$\mathbb{F}_q$ の適当な拡大の中で，1 の原始 p 乗根 w を考える．$w^p = 1$ であるから，w^x は $x \in \mathbb{F}_p$ に対して定まる．そして，Legendre 記号 $\left(\frac{x}{p}\right)$ を $x \in \mathbb{F}_p^*$ に対しても考えることができる．なぜならば $\left(\frac{d}{p}\right)$ は明らかに法 p に関する d の剰余類にのみ依存するからである．$a \in \mathbb{F}_p^*$ に対して「Gauss 和」，すなわち

$$\tau(a) = \sum_{x \in \mathbb{F}_p^*} \left(\frac{x}{p}\right) w^{ax} \tag{3}$$

を考える．$\tau(a)$ は $\mathbb{F}_q$ のある拡大体の元である．$ax = y$ とおくと，(2) より

$$\tau(a) = \sum_{y \in \mathbb{F}_p^*} \left(\frac{ya^{-1}}{p}\right) w^y = \left(\frac{a^{-1}}{p}\right) \sum_{y \in \mathbb{F}_p^*} \left(\frac{y}{p}\right) w^y$$

となり，よって

$$\tau(a) = \left(\frac{a}{p}\right) \tau(1) \tag{4}$$

を得る．他方，標数 q の体で考えていることと，$\left(\frac{x}{p}\right) \in \mathbb{F}_q$ であることから，

$$\tau(1)^q = \sum_{x \in \mathbb{F}_p^*} \left(\frac{x}{p}\right) w^{qx}$$

であり，よって q と q の法 p での剰余とを同一視して，

$$\tau(1)^q = \tau(q) \tag{5}$$

を得る．$\tau(1)^2$ を計算してみよう．

$$\tau(1)^2 = \sum_{x,y \in \mathbb{F}_p^*} \left(\frac{x}{p}\right)\left(\frac{y}{p}\right) w^{x+y}$$

が成り立つ．$y = tx$ とおくと，

$$\tau(1)^2 = \sum_{x,t\in\mathbb{F}_p^*} \left(\frac{x}{p}\right)^2 \left(\frac{t}{p}\right) w^{x(1+t)}$$

$$= \sum_{x,t} \left(\frac{t}{p}\right) w^{x(1+t)} = \sum_{t\in\mathbb{F}_p^*} \left(\left(\frac{t}{p}\right) \sum_{x\in\mathbb{F}_p^*} w^{x(1+t)} \right).$$

がわかる．もし $w^{1+t} \neq 1$ ならば，等比数列の和の公式より $\sum_{j=0}^{p-1}(w^{1+t})^j = 0$ となる．$(w^{1+t})^0 = 1$ であるから，もし $w^{1+t} \neq 1$ ならば

$$\sum_{x\in\mathbb{F}_p^*} w^{x(1+t)} = -1$$

である．もし $w^{1+t} = 1$ ならば，$\sum_{x\in\mathbb{F}_p^*} w^{x(1+t)} = p-1$ である．w が 1 の原始 p 乗根であるから，これは $t=-1$ のとき，そのときに限って起きる．従って

$$\tau(1)^2 = \left(\frac{-1}{p}\right)(p-1) - \sum_{t\in\mathbb{F}_p^*, t\neq -1} \left(\frac{t}{p}\right).$$

$\mathbb{F}_p^*$ においては非平方なものは平方なものと同数存在するから，$\sum_{t\in\mathbb{F}_p^*} \left(\frac{t}{p}\right) = 0$ である．よって

$$\tau(1)^2 = \left(\frac{-1}{p}\right)(p-1) + \left(\frac{-1}{p}\right) = \left(\frac{-1}{p}\right)p.$$

Euler の判定法（命題 1）より，

$$\tau(1)^2 = (-1)^{\frac{p-1}{2}} p \tag{6}$$

を得る．最後に，(4) と (5) を用いて，

$$\tau(1)^q = \tau(q) = \left(\frac{q}{p}\right)\tau(1)$$

がわかる．(6) より $\tau(1) \neq 0$ で，簡略化すれば

$$\tau(1)^{q-1} = \left(\frac{q}{p}\right)$$

となる．(6) を再度用いて，

$$\left(\frac{q}{p}\right) = (\tau(1)^2)^{\frac{q-1}{2}} = (-1)^{\frac{(p-1)(q-1)}{4}} p^{\frac{q-1}{2}}$$

を得る．$p^{\frac{q-1}{2}} = \left(\frac{p}{q}\right)$（命題 1）と $\left(\frac{p}{q}\right) = \left(\frac{p}{q}\right)^{-1}$ であることより，平方剰余の相互法則が証明された．□

命題 2（補充公式）． p を奇素数とすれば

(a) $\left(\dfrac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$,

(b) $\left(\dfrac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

証明　関係 (a) は Euler の判定法（命題 1）の特別の場合である．(b) を証明すればよい．まず，$1, 3, 5, 7$ の法 8 での平方は $1, 1, 1, 1$ であるから，$p^2 \equiv 1 \pmod 8$ である．よって (b) は意味をもつことに注意する．次に，環 $\mathbb{Z}/8\mathbb{Z}$ の単数の群 $H = \{1, 3, 5, 7\}$ においては，$\{1, 7\}$ は指数 2 の部分群 H' である．$x \in H'$ に対して $\theta(x) = 1$，$x \in H \setminus H'$ に対して $\theta(x) = -1$ とおくと $\theta(xy) = \theta(x)\theta(y) \quad (x, y \in H)$ が成り立つ．w を $\mathbb{F}_p$ のある拡大における 1 の原始 8 乗根とする．定理 1 のときのように，$a \in H$ に対して「Gauss 和」

$$\tau(a) = \sum_{x \in H} \theta(x) w^{ax} \tag{7}$$

を考える．定理 1 のときのように，$\tau(a) = \theta(a)\tau(1), \tau(1)^p = \tau(p)$（$p$ と p の法 8 での剰余類を同一視している）が成り立つことがわかる．$w^8 = 1, w^4 = -1$ であるから，$\theta(x)$ の定義より，

$$\begin{aligned}\tau(1) &= w - w^3 - w^5 + w^7 \\ &= (1 - w^2)(w - w^5) \\ &= w(1 - w^2)(1 - w^4) \\ &= 2w(1 - w^2)\end{aligned}$$

を得る．従って

$$\tau(1)^2 = 4w^2(1 - 2w^2 + w^4) = -8w^4 = 8$$

である．定理 1 のときのように

$$\tau(1)^p = \tau(p) = \theta(p)\tau(1)$$

が示される．次に

$$\theta(p) = (\tau(1)^2)^{\frac{p-1}{2}} = 8^{\frac{p-1}{2}} = \left(\frac{8}{p}\right) \quad \text{（命題 1）}$$
$$= \left(\frac{2}{p}\right)^3 = \left(\frac{2}{p}\right)$$

がわかる．従って，$\left(\frac{2}{p}\right) = \theta(p)$ である．さて，$x = 1,\ 3,\ 5,\ 7$（またはより簡単に，$x = 1,\ 3,\ -3,\ -1$）を代入して直接計算することにより，$\theta(x) = (-1)^{\frac{x^2-1}{8}}$ であることと $(-1)^{\frac{x^2-1}{8}}$ が x の法 8 での剰余にのみ依存することが示される．　□

例　相互法則の応用． 平方剰余の相互法則と補充公式を使って一連の簡約化をすることにより Legendre 記号を計算することが可能となる．$\left(\frac{23}{59}\right)$ を法 59 に関しての平方を計算することなしで求めてみよう．

$$\begin{aligned}
\left(\frac{23}{59}\right) &= (-1)^{11\cdot 29}\left(\frac{59}{23}\right) \\
&= -\left(\frac{13}{23}\right) \\
&= -(-1)^{6\cdot 11}\left(\frac{23}{13}\right) \\
&= -\left(\frac{10}{13}\right) \\
&= -\left(\frac{-3}{13}\right) \\
&= -\left(\frac{-1}{13}\right)\left(\frac{3}{13}\right) \\
&= -(-1)^{6}\left(\frac{3}{13}\right) \\
&= -(-1)^{6\cdot 1}\left(\frac{13}{3}\right) \\
&= -\left(\frac{1}{3}\right) \\
&= -1.
\end{aligned}$$

従って 23 は法 59 で平方でない．

5.6　2 平方和の定理

5.4 節の命題 1 を体 $L = \mathbb{Q}[i]$ $(i^2 = -1)$ に適用してみよう．$-1 \equiv 3 \pmod 4$ であることより，L の整数環 B は $\mathbb{Z} + \mathbb{Z}i$ である（2.5 節定理 1）．この環は **Gauss の整数環** (ring of Gaussian integer) といわれる．その判別式は -4（5.3 節例）である．p が奇素数で，u が巡回群 $\mathbb{F}_p^*$ の生成元であるとすれば，$-1 = u^{\frac{p-1}{2}}$ である．従って，-1 が $\mathbb{F}_p$ において平方数であるためには $\frac{1}{2}(p-1)$ が偶数であることが必要十分である．そこで次のような素数の分類を得る．

- 2 は $\mathbb{Q}[i]$ で分岐する，
- $4k+1$ の形の素数は分解する，
- $4k+3$ の形の素数は素を保つ．

次の結果は有益であろう．

命題 1. Gauss の整数環 $B = \mathbb{Z}[i] = \mathbb{Z} + \mathbb{Z}i$ は単項イデアル環である．

証明　このやさしい命題を証明するために以前の結果を大いに利用する．4.3 節の記号の下で，$n = 2$, $r_1 = 0$, $r_2 = 1$, $d = -4$ の場合にあたる．従って，B のすべてのイデアル類はノルムが $(4/\pi)(2/4)|4|^{\frac{1}{2}} = 4/\pi$ 以下の整イデアルを含む（4.3 節命題 1 の系）．よって B のすべてのイデアル類は単数イデアル B 自身を含む．B はノルムが 1 となる唯 1 つの整イデアルである（$4/\pi < 2$ に注意する）．よって B のすべてのイデアルは単項イデアル $B \cdot 1$ と同値である．ゆえに B は単項イデアル環である．　□

∞ **初等的証明の概略.** B の点は $\mathbb{Z}^2 \subset \mathbb{R}^2 \subset \mathbb{C}$ と同一視できる．$\mathbb{R}^2$ をいつものように平面（Euclid の距離の平方は $\mathbb{Q}[i]$ におけるノルムである）と同一視すると，$\mathbb{Z}^2$ の点は平面を覆う正方形の頂点になる．少し幾何的に見てみると，任意の $x \in \mathbb{Q}[i]$ に対して，$z \in B$ で $\mathrm{N}(x-z) = |x-z|^2 \leq (1/\sqrt{2})^2 = 1/2 < 1$ となるものが存在する．さて (0) でない B のイデアル $\mathfrak{a}$ の中で，ノルムが最小となる 0 でない元 u を選ぶ（注意．ノルムは $\mathbb{Z}[i] \setminus (0)$ 上の正整数値

をとる関数である）．任意の $v \in \mathfrak{a}$ に対して $\mathrm{N}(v/u - z) < 1$ となる $z \in B$ が存在する．従って，$\mathrm{N}(v - zu) < \mathrm{N}(u)$ となり，$v - uz = 0$ である（なぜなら $v - zu \in \mathfrak{a}$ であるから）．結局，$v \in uB$ となり $\mathfrak{a} = uB$ を得る．読者は $\mathbb{Z}$ が単項イデアル環であることの証明（1.1 節）と類似していることに気がつくであろう．

命題 2 (Fermat). 任意の素数 $p \equiv 1 \pmod 4$ は 2 つの平方の和（すなわち，$p = a^2 + b^2$ $(a, b \in \mathbb{N})$ の形）で表される．

証明 $B = \mathbb{Z} + \mathbb{Z}i$ (Gauss 環) とすると，実は pB は $pB = \mathfrak{p}_1\mathfrak{p}_2$ という 2 つの素イデアルの積である．明らかに $p^2 = \mathrm{N}(pB) = \mathrm{N}(\mathfrak{p}_1)\mathrm{N}(\mathfrak{p}_2)$（3.5 節命題 2）である．$\mathfrak{p}_1$ と $\mathfrak{p}_2$ のノルムは 1 より大きいから，必然的に $\mathrm{N}(\mathfrak{p}_1) = \mathrm{N}(\mathfrak{p}_2) = p$ となる．ここで，$\mathfrak{p}_1$ は単項イデアル $(a + bi)B$ $(a, b \in \mathbb{Z})$（命題 1）であるから，$p = \mathrm{N}(a + bi) = a^2 + b^2$ である． □

定理 1. x を自然数として，$x = \prod_p p^{v_p(x)}$ を素因数分解とする．x が 2 つの平方数の和で表せるためには，すべての $p \equiv 3 \pmod 4$ に対して，指数 $v_p(x)$ が偶数であることが必要十分条件である．

証明　（十分性）2 つの平方数の和 $a^2 + b^2$ は Gauss の整数環 B の元のノルム $\mathrm{N}(a + bi)$ であることに注意する．ノルムが乗法的であることにより，2 つの平方数の和の集合 S は乗法に関して閉じている．$2 = 1^2 + 1^2 \in S$ かつ任意の平方数も S の元である（$x^2 = x^2 + 0^2$ である）から，十分性は命題 2 より出る．

（必要性）$x = a^2 + b^2 = (a + bi)(a - bi)$ を 2 つの平方の和 $(a, b \in \mathbb{N})$ とし，p を $p \equiv 3 \pmod 4$ である素数とする．B のイデアル pB は素イデアルである（5.4 節命題 1）．$(a + bi)B$ を素イデアルの積で表したときのイデアル pB の指数を n とする．pB は B の自己同型 $\sigma : u + vi \mapsto u - vi$ について不変であることと，$\sigma(a + bi) = a - bi$ であることより，$(a - bi)B$ を素イデアルの積で表したときの pB の指数もまた n である．従って，$(a^2 + b^2)B$ を素イデアルの積で表わしたときの pB の指数は $2n$ である．p 以外のどの素数も pB に属さない（なぜならば $pB \cap \mathbb{Z} = p\mathbb{Z}$ だから）ことより，$v_p(x) = 2n$ であり，$v_p(x)$ は偶数である． □

5.7　4 平方和の定理

この節においては，次の定理を証明するのが目的である．

定理 1 (Lagrange)．すべての自然数は 4 つの平方数の和で表される．

この証明の背後にある考え方は 5.6 節の考え方に似ている，すなわち，Gauss の整数環の代わりに，適当に選んだ**四元数** (quaternion) の環を扱う．

四元数の定義から始めよう．環 A が与えられたとき，$\{1, i, j, k\}$ で A-加群 A^4 の標準的基底を表し，A^4 における乗法を次のように定義する．

$$\begin{cases} 1 \text{ は単位元}, \\ i^2 = j^2 = k^2 = -1, \\ ij = -ji = k,\ jk = -kj = i,\ ki = -ik = j. \end{cases} \tag{1}$$

この乗法を線型的に A^4 の元 $a + bi + cj + dk$ に拡張する．分配律は明らかである．基底の元に対する結合律を確認すれば十分である．たとえば，

$$i(jk) = i^2 = -1 = k^2 = (ij)k$$

である．1 の現れる等式は明らかであるから，$3^3 - 1 = 26$ 個の等式を調べることが残っている．忍耐強くて疑い深い読者は，入れ換えを考えて等式の個数を節約し，残りのものを調べるであろう．そうでない読者は与えられた乗法が結合律をみたすという著者の主張を受け入れればよい．この乗法が与えられたとき，A^4 は必ずしも可換環にはならないが A-代数にはなる．これを A 上の**四元数環** (algebra of quaternions) といい，$\mathbb{H}(A)$ と表す（$\mathbb{H}$ は四元数を考え出した W. R. Hamilton にちなんでいる）．

A 上の四元数 $z = a + bi + cj + dk$（$a \cdot 1$ の代わりに a と表す）に対して，z の**共役な** (conjugate) 四元数を $\overline{z} = a - bi - cj - dk$ と定義する．

補題 1.　$z, z' \in \mathbb{H}(A)$ に対して，$\overline{z + z'} = \overline{z} + \overline{z'}$,　$\overline{zz'} = \overline{z'}\,\overline{z}$,　$\overline{\overline{z}} = z$ が成り立つ．言い換えると $z \mapsto \overline{z}$ は $\mathbb{H}(A)$ の**対合的反自己同型** (involutive antiautomorphism) である．

証明　第 1 と第 3 の式は明らかである．線型性により，第 2 の式を証明す

るためには，$x, y \in \{1, i, j, k\}$ に対して $\overline{xy} = \overline{y} \cdot \overline{x}$ を調べれば十分である．$x = 1$ または $y = 1$ のときは，これは明らかである．$x = y = i$ のときは $\overline{xy} = \overline{-1} = -1$，$\overline{y} \cdot \overline{x} = (-i)(-i) = i^2 = -1$．

$x = i, y = j$ のときは

$$\overline{xy} = \overline{k} = -k, \quad \overline{y} \cdot \overline{x} = (-j)(-i) = ji = -k$$

である．他のものは入れ換えを考えればよい．□

A 上の四元数 z が与えられたとき，四元数 $\mathrm{N}(z) = z\overline{z}$ を z の**被約ノルム** (reduced norm) という．

補題 2. 次のことが成り立つ．

(a) $z = a + bi + cj + dk \in \mathbb{H}(A)$ について $\mathrm{N}(z) = a^2 + b^2 + c^2 + d^2$（4 平方！）で，$\mathrm{N}(z) \in A$ である．

(b) $z, z' \in \mathbb{H}(A)$ について，$\mathrm{N}(zz') = \mathrm{N}(z)\mathrm{N}(z')$．

証明　(a) を証明するには，$(a + bi + cj + dk)(a - bi - cj - dk)$ の展開式で等式 (1) を用いると，交差積の項は相殺されてしまい，$a^2 + b^2 + c^2 + d^2$ だけが残ることを確認すればよい．(b) を証明するためには，$\overline{z}z = z\overline{z}$ より，

$$\mathrm{N}(zz') = zz'\overline{zz'} = zz'\overline{z'}\overline{z} = z\mathrm{N}(z')\overline{z} = z\overline{z}\mathrm{N}(z')$$

を確認すればよい．($\mathrm{N}(z') \in A$ で，A の任意の元はすべての四元数と可換であるから）．よって $\mathrm{N}(zz') = \mathrm{N}(z)\mathrm{N}(z')$ が成り立つ．□

∞ 補題 2 は（可換）環 A に対して，A 上の四元数の被約ノルム，すなわち，4 平方の和の集合は乗法に関して閉じていることを示している．

さて，四元数の代数 $\mathbb{H}(\mathbb{Q})$，非可換な部分環 $\mathbb{H}(\mathbb{Z})$ と **Hurwitz の四元数**とよばれる部分集合 $\mathbb{H}$（すなわち，$a+bi+cj+dk$ の形の四元数で，$a, b, c, d \in \mathbb{Z}$ または $a, b, c, d \in \frac{1}{2} + \mathbb{Z}$ であるもの全体）について，より詳しく調べてみよう．

補題 3. 次のことが成り立つ．

(a) Hurwitz の四元数の集合 $\mathbb{H}$ は $\mathbb{H}(\mathbb{Z})$ を含む $\mathbb{H}(\mathbb{Q})$ の非可換の部分環であり，共役をとること $(z \mapsto \overline{z})$ に関して閉じている．

(b) 任意の $z \in \mathbb{H}$ に対して，$z + \overline{z} \in \mathbb{Z}, \mathrm{N}(z) = z\overline{z} \in \mathbb{Z}$ である．

(c) $z \in \mathbb{H}$ が可逆であるためには $\mathrm{N}(z) = 1$ であることが必要十分である．

(d) $\mathbb{H}$ のすべての左イデアル（あるいは，右イデアル）$\mathfrak{a}$ は単項イデアル，すなわち，$\mathbb{H}z$ （あるいは，$z\mathbb{H}$）の形である．

証明 (a) においては，$\mathbb{H}$ が乗法に関して閉じていること以外は明らかである．(a) の証明を完全にするためには，

$$u = \frac{1}{2}(1 + i + j + k)$$

とおいて，$u \cdot 1$, $u \cdot i$, $u \cdot j$, $u \cdot k$, $u^2 \in \mathbb{H}$ を示せば十分である．そして，

$$\begin{aligned}
u \cdot 1 &= \frac{1}{2}(1 + i + j + k), \\
u \cdot i &= \frac{1}{2}(-1 + i + j - k), \\
u \cdot j &= \frac{1}{2}(-1 - i + j + k), \\
u \cdot k &= \frac{1}{2}(-1 + i - j + k)
\end{aligned}$$

が成り立ち，これらはすべて $\mathbb{H}$ の元であることがわかる．さらに

$$2u^2 = \frac{1}{2}(-2 + 2i + 2j + 2k)$$

であり，よって $u^2 \in \mathbb{H}$ もわかる．

(b) については

$$z = \frac{1}{2} + a + \left(\frac{1}{2} + b\right) i + \left(\frac{1}{2} + c\right) j + \left(\frac{1}{2} + d\right) k \quad (a, b, c, d \in \mathbb{Z})$$

とおくと

$$\begin{aligned}
z + \overline{z} &= 1 + 2a \in \mathbb{Z}, \\
z\overline{z} &= \left(\frac{1}{2} + a\right)^2 + \left(\frac{1}{2} + b\right)^2 + \left(\frac{1}{2} + c\right)^2 + \left(\frac{1}{2} + d\right)^2 \\
&\in \frac{4}{4} + \mathbb{Z} \subset \mathbb{Z} \quad \text{（補題 2(b)）}
\end{aligned}$$

となる．

もし z が $\mathbb{H}$ で可逆であって，$z' = z^{-1}$ であるならば，

$$\mathrm{N}(z)\mathrm{N}(z') = \mathrm{N}(zz') = 1$$

となる．$\mathrm{N}(z)$ と $\mathrm{N}(z')$ はともに正の整数（(b) と補題 2(a)）であることより，$\mathrm{N}(z) = 1$ である．逆に，$z \in \mathbb{H}$ で $\mathrm{N}(z) = 1$ ならば，

$$z\overline{z} = \overline{z}z = \mathrm{N}(z) = 1$$

となり，(a) より $\overline{z} \in \mathbb{H}$ なので，z は $\mathbb{H}$ で可逆である．これで (c) が示せた．

(d) を証明するために，

$$x = a + bi + cj + dk \in \mathbb{H}(\mathbb{Q})$$

をとる．$a', b', c', d' \in \mathbb{Z}$ で

$$|a - a'| \leq \frac{1}{2}, \quad |b - b'| \leq \frac{1}{2}, \quad |c - c'| \leq \frac{1}{2}, \quad |d - d'| \leq \frac{1}{2}$$

となるものが存在する．$z = a' + b'i + c'j + d'k$ とおく．このとき，

$$\mathrm{N}(x - z) = (a - a')^2 + (b - b')^2 + (c - c')^2 + (d - d')^2 \leq 4 \cdot \frac{1}{4} = 1$$

である．

a, b, c, d がすべて $\frac{1}{2} + \mathbb{Z}$ に属する場合（このときは $x \in \mathbb{H}$）を除いて，この不等式は完全に等号となる．よって，任意の四元数 $x \in \mathbb{H}(\mathbb{Q})$ に対して，Hurwitz の四元数 $z \in \mathbb{H}$ が存在して，$\mathrm{N}(x - z) < 1$ （真の不等式をとらないければならないことが，Hurwitz の四元数を扱う理由なのであって，$\mathbb{H}(\mathbb{Z})$ では十分でないのである）となる．さて，$\mathfrak{a}$ を $\mathbb{H}$ の左イデアルとする．$\mathfrak{a}$ が単項イデアルであることを示すためには $\mathfrak{a} \neq (0)$ としてよい．$\mathfrak{a}$ の中に 0 でない元 u で $\mathrm{N}(u)$ が最小のものをとる（被約ノルムは $\mathbb{H} \setminus (0)$ 上の正の整数値をとる関数であるから，(b) により，そのような元 u は存在する）．明らかに，u は $\mathbb{H}(\mathbb{Q})$ では逆元 $\overline{u}\mathrm{N}(u)^{-1}$ をもつので可逆である（このことは $\mathbb{H}(\mathbb{Q})$ が斜体 (skew field) であることを示している）．$y \in \mathfrak{a}$ に対して，$yu^{-1} \in \mathbb{H}(\mathbb{Q})$ を考え，元 $z \in \mathbb{H}$ を $\mathrm{N}(yu^{-1} - z) < 1$ であるようにとる．このとき補題 2(b) より，

$$\mathrm{N}(y - zu) = \mathrm{N}((yu^{-1} - z)u) < \mathrm{N}(u)$$

がわかる．$y-zu \in \mathfrak{a}$ で $\mathrm{N}(u)$ は可能な限り小さくとってあるから，$y-zu=0$ でなければならない．よって $y \in \mathbb{H}u$ となり，$\mathfrak{a}=\mathbb{H}u$ がいえる． □

さて，定理 1 を証明する準備ができた．4 つの平方数の和である $\mathbb{Z}$ の元全体の集合は乗法に関して閉じている（補題 2 を参照）から，定理 1 は次の命題から得られる．

命題 1． 任意の素数は 4 つの平方数の和で表される．

証明 $2=1^2+1^2+0^2+0^2$ であるから，素数 p は奇数としてよい．p は任意の四元数と可換であるから，左イデアル $\mathbb{H}p$ は両側イデアルである．剰余環 $\mathbb{H}/\mathbb{H}p$ を考える．p は奇素数であるから，任意の $z \in \mathbb{H}$ は $\mathbb{H}p$ を法として $\mathbb{H}(\mathbb{Z})$ の元と合同である（もし z の係数がすべて $\frac{1}{2}+\mathbb{Z}$ に属しているならば，$z+p\cdot\frac{1}{2}(1+i+j+k)$ を考えればよい）．従って，$\mathbb{H}/\mathbb{H}p$ は $\mathbb{H}(\mathbb{Z})$ の剰余環（すなわち $\mathbb{H}(\mathbb{F}_p)$）に同型になる．

2 次形式 $a^2+b^2+c^2+d^2$ は $\mathbb{F}_p$ においては 0 を表す（1.7 節定理 2，または直接の証明としては以下の注意を参照せよ）から，$\mathbb{H}(\mathbb{F}_p)$ は被約ノルムが 0 である 0 でない元を含む．そのような元は可逆ではない（補題 2(b)）ので，その元は自明でない左イデアルを生成する．これより，$\mathbb{H}p$ は $\mathbb{H}$ と異なるある左イデアル $\mathbb{H}z$ に真に含まれる．従って，ともに単元でない元 $z, z' \in \mathbb{H}$ により，$p=z'z$ と書ける．よって

$$p^2=\mathrm{N}(p)=\mathrm{N}(z)\mathrm{N}(z')$$

となる．$\mathrm{N}(z), \mathrm{N}(z')$ はともに 1 より大きい整数（補題 3(b)，(c)）であるから，$\mathrm{N}(z)=\mathrm{N}(z')=p$ を得る．

$z=a+bi+cj+dk$（$a,b,c,d \in \mathbb{Z}$ または $\in \frac{1}{2}+\mathbb{Z}$）とおく．もし $a,b,c,d \in \mathbb{Z}$ ならば $p=\mathrm{N}(z)=a^2+b^2+c^2+d^2$ となり，証明は終わる．$a,b,c,d \in \frac{1}{2}+\mathbb{Z}$ とするとき，被約ノルムが 1 の $\mathbb{H}$ の元，より詳しくいうと $\frac{1}{2}(\pm1\pm i\pm j\pm k)$ の形の元を z に掛けて，前述の場合に帰着できることを示せば十分である．そのために，$\mathbb{H}(\mathbb{Z})/4\mathbb{H}(\mathbb{Z}) \cong \mathbb{H}(\mathbb{Z}/4\mathbb{Z})$ の中で $2z$ を含む剰余類 η を考える．$\mathrm{N}(z) \in \mathbb{Z}$ であるから，$\mathrm{N}(2z) \in 4\mathbb{Z}$．よって $\mathrm{N}(\eta)=0$ となり，$\eta\overline{\eta}=0$ がわかる．$\overline{\eta}$ は $\pm1\pm i\pm j\pm k$ の形の四元数 z'

の剰余類である．$u = \frac{1}{2}z' \in \mathbb{H}$ とおくと，u は被約ノルム 1 をもち，さらには $(2z)(2u) \equiv 0 \pmod 4$ であることより，$zu \in \mathbb{H}(\mathbb{Z})$ である．こうして $p = \mathrm{N}(z) = \mathrm{N}(zu)$ であるから証明は完了した．□

∞ **注意．** 有限体 K 上で，2 次形式 $a^2+b^2+c^2+d^2$ が 0 を表す（すなわち，K^4 で自明でない零点をもつ）ということのとても初等的な証明がある．$c=1, d=0$ ととって，方程式 $a^2+b^2+1=0$ が K^2 で解をもつことを示せば十分である．この方程式を $b^2+1=-a^2$ の形に書く．標数 2 のときは，$b=0, a=1$ ととればよい．$\mathrm{card}(K)=q$ が奇数とすれば，K の中に $(q+1)/2$ 個の平方数（0 と $(q-1)/2$ 個の 0 でない平方数）がある．よって b^2+1 $(b \in K)$ の形（あるいは，$-a^2$ $(a \in K)$ の形）の K の元全体の集合 T（あるいは，T'）は $(q+1)/2$ 個の元からなる．$(q+1)/2+(q+1)/2>q$ であるから，$T \cap T' \neq \emptyset$ であり，$b^2+1=-a^2$ は解をもつ．

練習問題

1*. A を単項イデアル環，K をその分数体とする．
(a) 任意の中間体 B $(A \subset B \subset K)$ は A の分数環であることを示せ（ヒント：$a/b \in B$（$a, b \in A$ は互いに素）ならば，Bezout の等式を用いて，$1/b \in B$ を得る）．
(b) A の分数環を分類せよ（ヒント：A の素元で $S^{-1}A$ において可逆元となるもの全体を考えよ）．
(c) A の任意の分数環は単項イデアル環であることを示せ．

2. 8 を法として 7 と合同な整数は 3 つの平方数の和で書けない（ヒント：8 を法として簡約化する）．

3*. K は体，A を K 上有限次元の被約な K-代数とする．
(a) 5.3 節の補題 3 を用いて，A は K の有限拡大体の有限個の直積 $\prod_{i=1}^{n} L_i$ に同型であることを示せ．
(b) K が標数 0 ならば，A は原始生成元をもつ，すなわち，A は $K[x]$ $(x \in A)$ の形であることを示せ（ヒント：K 上の体 L_i の原始生成元 x_i で，その K 上の最小多項式が互いに異なるようなものの集合を見つける．$x = \{x_1, \ldots, x_n\}$ をとる）．

4*. p を素数で，$p \equiv 1 \pmod 4$ であるとする．組 $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ で $a^2 + b^2 = p$ となるものはちょうど 8 組あることを示せ（ヒント：Diophantus 方程式 $p = a^2 + b^2$ は自明な変換を除いて唯 1 つの解 (a, b) をもつ）．

5*. K を体，A を K 上の有限次元の K-代数とする．A が原始生成元をもたない（すなわち，$K[x]$ の形でない）ような例をあげよ．
(a) A が被約でないとき．
(b) A は被約で K は有限体であるとき（問題 3 を参照）．

6*. (a) 多項式 $X^5 - X + 1$ は $\mathbb{Q}$ 上既約であることを示せ（ヒント：これらの 5 を法とする簡約化を見てみる）．x をこの多項式の根の 1 つとする．$\mathbb{Q}[x]$ について，整数 r_1 と r_2 を計算せよ．
(b) $(1, x, \ldots, x^4)$ の判別式を計算せよ（ヒント：$\mathbb{Z}$ 上．2.7 節公式 (7) を参照）．この判別式は平方因子をもたないことを示し，$\mathbb{Z}[x]$ が $\mathbb{Q}[x]$ の整数環であることを導け（ヒント：5.3 節命題 1）．
(c) 環 $\mathbb{Z}[x]$ は単項イデアル環であることを示せ（ヒント：4.3 節の命題 1 の系 1 を用いる．法 2，法 3 での $X^5 - X + 1$ の簡約化により，$\mathbb{Z}[x]$ がノルムが 2 または 3 となるイデアルを含まないことに注意する）．

7*. $K=\mathbb{Q}[\sqrt{d}]$ を 2 次体で，d は平方因子をもたない整数，A は K の整数環とする．

(a) 4.3 節の系 1 によって，$d=2,3,5,13,-1,-2,-3,-7$ のときは，A は単項イデアル環になることを示せ．

(b) 同じ方法で，$d=6,7,17,21,29,33,-5,-11,-15,-19$ のときは，K の任意のイデアルはノルムが 1 または 2 の整イデアルと同値であることを示せ．上記の体において 2 が素を保つ（$d=21,29,-11,-19$．5.4 節命題 1 を参照）ものはどれか？その整数環は単項イデアル環であることを示せ．

(c) $d\equiv 2$ または $3 \pmod 4$ とする．K がノルム 2 となる単項イデアルを含むための必要十分条件はある $a,b\in\mathbb{Z}$ が存在して $a^2-db^2=\pm 2$ となることであることを示せ．$d=6,7$ に対しては A は単項イデアル環であること，そして $d=-5$ のときは A は 2 つのイデアル類をもつことを導け（ヒント：2 はこの体では分岐することに注意する）．

(d) $d\equiv 1 \pmod 4$ とする．K がノルムが 2 の単項イデアルを含むための必要十分条件は $a^2-db^2=\pm 8$ が解 $(a,b)\in\mathbb{Z}\times\mathbb{Z}$ をもつことであることを示せ．$d=17,33$ のとき A は単項イデアル環であること，$d=-15$ のときは A は 2 つのイデアル類をもつことを導け（ヒント：2 はこの体では分解することに注意する）．

(e) $d=10$ と $d=-6$ については，A は 2 つのイデアル類をもつことを示せ（ヒント：K の任意のイデアルはノルムが 1,2 または 3 の整イデアルと同値であることに注意する．K における 2 と 3 の分解を調べて，$(2+\sqrt{10})(2-\sqrt{10})=-2\cdot 3$，$(\sqrt{-6})^2=-2\cdot 3$ を示す）．

(f) $d=-23$ のときは，A は 3 つのイデアル類をもつことを示せ（ヒント：(e) のときのようにする．A の単項でない素イデアル $\mathfrak{p},\mathfrak{p}',\mathfrak{q},\mathfrak{q}'$ があって，$2A=\mathfrak{p}\mathfrak{p}'$，$3A=\mathfrak{q}\mathfrak{q}'$ となることを示す．$x=\frac{1}{2}(3+\sqrt{-23})$ と $y=\frac{1}{2}(1+\sqrt{-23})$ は A の元でノルムがそれぞれ 8 と 6 である．Ax と Ay の素イデアルの分解を調べる）．

8. K,K',K'' を数体で $K\subset K'\subset K''$ とする．$\mathfrak{p}''$ を K'' の極大イデアル，$\mathfrak{p}'=\mathfrak{p}''\cap K'$ とする．e（あるいは，e',e''）で $\mathfrak{p}''$ の K 上（あるいは $\mathfrak{p}'$ の K 上，$\mathfrak{p}''$ の K' 上）の分岐指数を表し，f（あるいは，f',f''）で $\mathfrak{p}''$ の K 上（あるいは $\mathfrak{p}'$ の K 上，$\mathfrak{p}''$ の K' 上）の剰余次数を表すものとする．このとき，$e=e'e''$，$f=f'f''$ であることを示せ．

9*. (a) 多項式 X^3+X^2-2X+8 は $\mathbb{Q}$ 上既約であることを示せ（ヒント：この多項式は $\mathbb{Z}$ の中では根をもたない，従って $\mathbb{Q}$ の中でももたないことに注意する）．x をこの多項式の根の 1 つとし，K を $\mathbb{Q}[x]$ とする．A を K の整数環とする．

(b) $D(1,x,x^2)=4\cdot 503$ で，503 は素数であることを示せ．

(c) $y=4/x$ は K の整数であり，$y\notin\mathbb{Z}[x]$ であることを示せ．$A'=\mathbb{Z}+\mathbb{Z}x+\mathbb{Z}y$ は K の部分環で $\mathbb{Z}[x]$ を真に含むことを示せ．A' の $\mathbb{Z}$ 上の判別式は 503 であるこ

とを示せ（ヒント：A と A' の判別式を比較するか，$D(1,x,y)$ を直接計算する）．$A=A'$ を結論づけよ．

(d) $2A$ は異なる 3 つの素イデアルの積であることを示せ（ヒント：$1,x,y$ の乗積表を書いて，2 を法として簡約化する）．このことより，A には $A=\mathbb{Z}[u]$ となる元 u は存在しないことを導け（ヒント：$A/2A$ は $\mathbb{F}_2$ 上原始的に生成されないことに注意する）．

(e) u が A に属する K の原始元ならば，群 $A/\mathbb{Z}[u]$ は位数 2 の剰余群をもつ（(d) で与えられた A の $\mathbb{F}_2$ 上への 3 つの準同型のうち 2 つは $\mathbb{Z}[u]$ 上では一致することに注意し，それらの違いを考える）．$D(1,u,u^2)$ は $4\cdot 503$ の倍数であることを結論づけよ（ヒント：$D(1,u,u^2)=503\cdot\mathrm{card}((A/\mathbb{Z}[u])^2)$ に注意する）．従って，すべての数 $D(1,u,u^2)$ について，$\mathbb{Q}$ のイデアルとしての K の判別式を生成しない．

(f) 環 A は単項イデアル環であることを示せ（ヒント：4.3 節の命題 1 の系 1 より，ノルム $n\leq 6$ となるすべての素イデアルが単項であることを示せば十分である．$n=6$ の場合を除外し，(d) を用いて $n=4$ の場合を除外する．それからノルムと $x,y,x-1,x+2,x+3$ の A の中での分解を調べる．$n=2$ のときを解決するために $(x-2)/(x+2)$ と $(x-1)/(x+3)$ はノルムが 2 となる 3 つの素イデアルのうちの 2 つを生成することを確認する．$n=3$ については $3A$ が素イデアルであることを示し，$n=5$ を解決するためには $5A$ はノルムが 5 とノルムが 25 である 2 つの素イデアルの積であることを示し，その分解と $5A$ と $(x+1)A$ のノルムを比較する）．

10*. (a) p,q を相異なる 5 以上の素数で，$pq^2\not\equiv 1 \pmod 9$ であるとする．K を 3 次体 $\mathbb{Q}[u]$，$u^3=p^2q$ とする．u と $v=pqu^{-1}$ は K の整数であること，$D(1,u,v)=-27p^2q^2$ であること，$B=\mathbb{Z}+\mathbb{Z}u+\mathbb{Z}v$ は K の整数環 A の部分環であることを示せ（ヒント：$u^2=qv$ と $v^2=pu$ に注意する）．

(b) $\mathfrak{q}$ を A の素イデアルで qA を含むものとする．$u^3=p^2q$ であることより，qA の分解における $\mathfrak{q}$ の指数は 3 であることと，$qA=\mathfrak{q}^3$ であることを導け．$B\cap\mathfrak{q}$ は u,v,q によって生成された B のイデアルであること，そして $A/\mathfrak{q}=B/B\cap\mathfrak{q}$ であること，そして $A=B+\mathfrak{q}$ であることを示せ．これより，$A=B+qA$ を結論づけよ．同様に，$pA=\mathfrak{p}^3$（$\mathfrak{p}$ は素イデアル）であることと，$A=B+pA$ であることを示せ．

(c) $(u\pm 1)^3$（これは p^2q の法 3 での類と 1 だけ差がある）を考えることにより，$3A$ が A の素イデアルの 3 乗であり，((b) のときのように）$A=B+3A$ となることを示せ．

(d) $x=a+bu+cv$ $(a,b,c\in\mathbb{Q})$ を K の整数とする．トレースを計算することにより，$3pqx\in B$ を導き，それより $3pqA\subset B$ となることを導け．(b) と (c) を用いて，$A=B+3pqA$ を示せ．これより $A=B$ を結論づけよ．

(e) $x=a+bu+cv$ $(a,b,c\in\mathbb{Z})$ に対して

$$D(1,x,x^2)=3p^2q^2(b^3q-c^3p)^2$$

であることを示せ．

(f) (e) より，$p\equiv 1 \pmod 3$ かつ $q^{(p-1)/3}\equiv 1 \pmod p$ ならば A は $\{1,x,x^2\}$ ($x\in A$) の形の $\mathbb{Z}$ 上の基底をもたないことを導け．$p=7, q=5$ のときがこの場合にあたることを示せ（ヒント：このとき $K=\mathbb{Q}[\sqrt[3]{175}]=\mathbb{Q}[\sqrt[3]{245}]$ である）．この場合，K の絶対判別式はすべての数 $D(1,x,x^2)$ ($x\in A$) の最大公約数であることを示せ．

第 VI 章　数体の Galois 拡大

6.1　Galois 理論

この節では 2.3，2.4，2.6，2.7 節で述べられた可換体の一般論を補足する．L を体，G を L の自己同型の集合とするとき，すぐわかることは，L の元 x で，すべての $\sigma \in G$ について $\sigma(x) = x$ が成り立つもの全体の集合は L の部分体をなすことである．この体を G の**不変体** (fixed field) という．また，体 K の拡大 L に対して，L の K-自己同型は写像の合成の下で群をなすことも明らかである．

定理 1. L を K の n 次の有限拡大，K は有限体または標数が 0 の体とする．次の条件は同値である．

(a) K は L の K-自己同型の群 G の不変体である．

(b) 任意の $x \in L$ について，x の K 上の最小多項式は L の中ですべての根をもつ．

(c) L は K に係数をもつ多項式のすべての根により生成される．

上の条件が成り立つとき，L の K-自己同型の群 G は位数 n である．

証明　(a) より (b) が示されることを見るために，$x \in L$ に対して多項式 $\prod_{\sigma\in G}(X - \sigma(x)) = P(X)$ が G で不変である（G の任意の元 τ は因数の

入れ換えをするだけであるから）ことを確認しよう*．従って $P(X)$ の係数は K に属する．x は $P(X)$ の根であるから（G は単位元を含む），x の最小多項式は $P(X)$ を割り切る（2.3 節 (4)）．ゆえに (a) より (b) が示される．

(b) から (c) を示すために，L の K 上の原始元 x をとる（2.4 節定理 1 の系）．(b) より x の K 上の最小多項式は L においてすべての根をもつ．明らかに，これらの根全体は K 上 L を生成する（任意の根がそうなので）．

最後に，(c) が (a) を示すことを見よう．仮定により L は K 上有限個の元 $\{x^{(1)}, \ldots, x^{(q)}\}$ とそのすべての共役元 $\{x_j^{(i)}\}$ により生成される（2.4 節）．L から L の拡大の中への任意の K-同型 σ は，これらの生成元を同じ集合の中の他の元に写すということは明らかである．従って $\sigma(L) \subset L$ である．さらに，σ は K-線型で単射であるから，線型代数の結果より $\sigma(L) = L$ を得る．言い換えると，σ は L の K-自己同型である．2.4 節の定理 1 より，L の K-自己同型の群 G はちょうど n 個の元をもつ．$x \in L$ を G で不変であるものとする．このとき，任意の $\sigma \in G$ は L の $K[x]$-自己同型になる．2.4 節の定理 1 より L から L の拡大体の中への $K[x]$-同型はちょうど $[L : K[x]]$ 個ある．よって $n \leq [L : K[x]]$．これより $n = [L : K[x]]$, $K[x] = K$, $x \in K$ という結論を得る．これは (c) が (a) を示すことを証明している．G の位数が n であることは途中で示されている．□

定義 1. 定理 1 の条件をみたすとき，L は K の **Galois 拡大**とよばれる．G は L の K 上の **Galois 群**とよばれる．もし G が Abel（あるいは，巡回）群のとき，L は K の **Abel**（あるいは，**巡回**）**拡大**であるという．

定理 1 の系. K を有限体または標数 0 の体，L を K の n 次の有限拡大，H を L の自己同型の群で K が H の不変体になるものとする．このとき，L は K の Galois 拡大で，H は L の K 上の Galois 群である．

証明 $x \in L$ に対して，多項式 $\prod_{\sigma \in H}(X - \sigma(x)) = P(X)$ は H で不変である．従って $P(X)$ は K の中に係数をもつ．x は $P(X)$ の根であるから，x の K 上の最小多項式は $P(X)$ を割り切る．定理 1(b) より，L は K の Galois 拡大

* G の有限性は 2.4 節の定理 1 よりわかる．

である．G を L の K 上の Galois 群とすると，$H \subset G$ であり，$\mathrm{card}(G) = n$ である（定理 1）．さて，x を L の K 上の原始元とし（2.4 節定理 1 の系），$P(X)$ を上で定義された多項式とする．$P(X) \in K[X]$ で，これは x の最小多項式で割り切れるから，$n \leq \deg(P)$ で $\deg(P) = \mathrm{card}(H) \leq \mathrm{card}(G) = n$ であることより $H = G$ であることがわかる． □

定理 2. K を有限体または標数 0 の体，L を K の Galois 拡大，G を L の K 上の Galois 群とする．G の任意の部分群 G' に対して G' の不変体 $k(G')$ を対応させ，L の K を含む任意の部分体 K' に対して L の K'-自己同型のなす G の部分群 $g(K')$ を対応させる．

(a) 写像 g と k は全単射で，一方は他方の逆写像になっている．g と k は G と L の中でのそれぞれの包含関係を互いに逆の包含関係に写す．さらに L は任意の中間体 K' の Galois 拡大である（すなわち，$K \subset K' \subset L$）．

(b) 中間体 K' が K の Galois 拡大であるためには $g(K')$ が G の正規部分群 (normal subgroup) であることが必要十分条件である．このとき，K' の K 上の Galois 群は剰余群 $G/g(K')$ と同一視できる．

証明 任意の中間体 K' と任意の $x \in L$ に対して，x の K' 上の最小多項式は x の K 上の最小多項式を割り切る．定理 1(b) によりその根はすべて L に属する．よって再度定理 1(b) によって，L は K' の Galois 拡大である．K' は L の K'-自己同型全体からなる群 $g(K')$ の不変体であり（定理 1(a)），言い換えると，$k(g(K')) = K'$ である．G' を G の部分群とする．このとき，G' は L の $k(G')$ 上の Galois 群であり（定理 1 の系），これは $G' = g(k(G'))$ を意味する．$k(g(K')) = K'$ と $g(k(G')) = G'$ という関係は，k と g が全単射で，一方が他方の逆写像であることを示している．明らかに，k と g は包含関係を逆にする．これで (a) は証明された．

(b) を示そう．K' を中間体 $(K \subset K' \subset L)$ とする．$x \in K'$ に対して x の K 上の最小多項式のすべての根は $\sigma(x)$ $(\sigma \in G)$ の形をしている L の元である．定理 1(b) によれば，K' が K の Galois 拡大であるためには，$\sigma(x) \in K'$ がすべての $x \in K'$ とすべての $\sigma \in G$ について成り立つこと，すなわち $\sigma(K') \subset K'$ がすべての $\sigma \in G$ について成り立つことが必要十分である．も

し $\sigma(K') \subset K', \tau \in g(K'), x \in K'$ ならば，$\sigma^{-1}\tau\sigma(x) = \sigma^{-1}\sigma(x) = x$ となり，$\sigma^{-1}\tau\sigma \in g(K')$ を得る．言い換えれば，K' が K 上 Galois 拡大であることは，$g(K')$ が G の正規部分群であることを示している．逆に，$g(K')$ が G の正規部分群とする．$x \in K', \sigma \in G, \tau \in g(K')$ ならば，$\sigma^{-1}\tau\sigma \in g(K')$ であるから，$\tau\sigma(x) = \sigma\sigma^{-1}\tau\sigma(x) = \sigma(x)$ である．よって $\sigma(x)$ は $g(K')$ のすべての元 τ で不変である．これより $\sigma(x) \in K'$ となる．ゆえに，$g(K')$ が G の正規部分群であることは，$\sigma(K') \subset K'$ を示しており，K' が K の Galois 拡大であることがわかる．

最後に，K' の K 上の Galois 群を決定しよう．$\sigma(K') \subset K'$ がすべての $\sigma \in G$ についていえる（線型代数によって $\sigma(K') = K'$ もいえる）から，σ の K' への制限 $\sigma|K'$ は K' の K-自己同型である．制限 $\sigma \mapsto \sigma|K'$ は，G から K' の K 上の Galois 群 H への準同型であり，明らかにその核は $g(K')$ である．$\mathrm{card}(H) = [K' : K] = [L : K]/[L : K'] = \mathrm{card}(G)/\mathrm{card}(g(K')) = \mathrm{card}(G/g(K'))$ であるから，この制限するという準同型は全射である．従って $H \cong G/g(K')$ となる．　□

例 1（2 次拡大）．K を標数 0 の体，L を K の 2 次拡大（すなわち，次数 2）とする．2.5 節の冒頭部分と同様にして，L は $K[x]$ の形をしていることがわかる．ここで x は多項式 $X^2 - d$（$d \in K$，d は K で平方ではない）の根である．この多項式の他の根は $-x$ であるから，$\sigma(x) = -x$ で定義される自明でない K-同型 σ，すなわち $\sigma(a+bx) = a - bx$ $(a, b \in K)$ が存在する．明らかに $\sigma^2 = 1$ で，K は σ の不変体である．よって L は K の Galois 拡大で，Galois 群は巡回群 $\{1, \sigma\}$ である（定理 1 とその系）．

例 2（円分体）．K を標数 0 の体，z を K の拡大の中での 1 の原始 n 乗根，$L = K(z)$ とする．体 L は K の**円分拡大** (cyclotomic extension) とよばれる．z の K 上の最小多項式 $F(X)$ は $X^n - 1$ を割り切る（2.3 節 (4)）．よって $F(X)$ の根は 1 の n 乗根であり，結局 z のべき（1.6 節）である．従って定理 1(c) により，L は K の Galois 拡大である．

G を L の K 上の Galois 群とする．任意の $\sigma \in G$ は z における作用 $\sigma(z)$ で定まる．より正確には，$\sigma(z)$ は z のべき $z^{j(\sigma)}$ である．ここで $j(\sigma)$

は n を法として一意的に決まる．$\sigma, \tau \in G$ に対して $\sigma\tau(z) = \sigma(z^{j(\tau)}) = \sigma(z)^{j(\tau)} = z^{j(\sigma)j(\tau)}$ であり，それゆえに

$$j(\sigma\tau) \equiv j(\sigma)j(\tau) \pmod{n}$$

であることがわかる．言い換えると，$\sigma \mapsto j(\sigma)$ は準同型 $G \to (\mathbb{Z}/n\mathbb{Z})^*$ を定義する．$j(\sigma)$ は σ を定めるから，この準同型は単射であって，G は Abel 群であることがわかる．従って,「任意の円分拡大は Abel 拡大」である．もし n が素数ならば，この拡大は巡回拡大でもある．なぜならば，G は $(\mathbb{Z}/n\mathbb{Z})^* = \mathbb{F}_n^*$ の部分群と同型であるからである（1.7 節定理 1(b)）．

☞ Abel 群の部分群は正規部分群であるから，円分拡大の中間体 K' は K の Galois 拡大（そして，Abel 拡大）である（定理 2(b)）．特に，円分体の任意の部分体は $\mathbb{Q}$ の Abel 拡大である．逆に，$\mathbb{Q}$ の任意の Abel 拡大は円分体の部分体であることを示すことができる（Kronecker-Weber の定理）．

前述の記号の下で，自己同型 σ はすべての 1 の n 乗根をその $j(\sigma)$ 乗に写すことがわかる．なぜならば，1 の n 乗根はすべて z のべきであるからである．よって $\sigma \mapsto j(\sigma)$ は z のとり方によらない．

例 3（有限体）．$\mathbb{F}_q$ を有限体（$q = p^s, p$ は素数）とする．$\mathbb{F}_q$ の任意の有限拡大は $\mathbb{F}_{q^n}$ の形である．その次数は n である（1.7 節）．写像 $\sigma : x \mapsto x^q$ は $\mathbb{F}_{q^n}$ の自己同型（同上，命題 1）で，$\mathbb{F}_q$ を不変体とする（同上，定理 1(c)）．任意の $x \in \mathbb{F}_{q^n}$ は $x^{q^n} = x$（同上，定理 1(c)）であるから，$\sigma^j(x) = x^{q^j}$ で $\sigma^n = 1$ となる．他方，もし $j < n$ ならば，ある $x \in \mathbb{F}_{q^n}$ があって $x^{q^j} \neq x$ となることより，$1 \leq j \leq n-1$ に対して，$\sigma^j \neq 1$ である．よって $\{1, \sigma, \ldots, \sigma^{n-1}\}$ は位数 n の巡回群である．定理 1 の系より，$\mathbb{F}_{q^n}$ は $\mathbb{F}_q$ の「n 次の巡回拡大」である．その Galois 群は標準的生成元として写像 $x \mapsto x^q$ をもつ．この写像は **Frobenius 自己同型**とよばれる．

6.2　分解群と惰性群

この節においては，A は Dedekind 環，K はその分数体（標数 0 とする），K' は K の n 次の Galois 拡大，G は K' の K 上の Galois 群，A' は A の

K' における整閉包とする．

A' の元 x の（A 上の）整従属方程式に $\sigma \in G$ を作用させて，$\sigma(x) \in A'$ を得る．従って

A'はGで安定している，すなわち，任意の$\sigma \in G$に対して$\sigma(A') = A'$．(1)

☞ $\sigma(A') \subset A'$ だけを示しておいた．なぜならば，$\sigma^{-1}(A') \subset A'$ でもあるので，$A' = \sigma\sigma^{-1}(A') \subset \sigma(A')$ となるからである．これ以後この種の議論の詳細は読者にゆだねることにする．

他方，$\mathfrak{p}$ を A の極大イデアルとし，$\mathfrak{p}'$ を A' の極大イデアルで $\mathfrak{p}' \cap A = \mathfrak{p}$ となるもの（すなわち，$\mathfrak{p}'$ は $\mathfrak{p}A'$ を A' において素イデアルの積に分解したときに現れる，5.2 節命題 1 を参照）とすれば，明らかに $\sigma(\mathfrak{p}') \cap A = \mathfrak{p}$ であり，$\sigma(\mathfrak{p}')$ もまた $\mathfrak{p}A'$ を A' において素イデアルの積に分解したときに現れるもので，$\mathfrak{p}'$ と同じ指数をもつ．$\mathfrak{p}'$ と $\sigma(\mathfrak{p}')$ は A' の**共役**な素イデアルという．$\mathfrak{p}A'$ を A' において素イデアル分解したときに現れるすべての素イデアルが共役であることを示そう．

命題 1． $\mathfrak{p}$ が A の極大イデアルならば，$\mathfrak{p}A'$ を A' において素イデアルの積で表したとき，そこに現れる A' のすべての極大イデアル $\mathfrak{p}'_i$（すなわち，極大イデアル $\mathfrak{p}'_i$ は $\mathfrak{p}'_i \cap A = \mathfrak{p}$ という性質で特徴づけられる）は共役である．それらはすべて同じ剰余次数 f と同じ分岐指数 e をもつ．従って $\mathfrak{p}A' = (\prod_{i=1}^{g} \mathfrak{p}'_i)^e$ かつ $n = efg$ である．

証明　自己同型はすべての代数的な関係を保存するから，分岐指数と剰余次数に関する主張は明らかである．従って等式 $n = efg$ は関係式 $\sum e_i f_i = n$（5.2 節定理 1）の特別の場合である．さて，$\mathfrak{p}'$ を $\mathfrak{p}'_i$ の 1 つとし，$\{\mathfrak{p}'_i\}$ の中の別の 1 つを $\mathfrak{q}'$ とする．また，$\mathfrak{q}'$ は $\mathfrak{p}'$ に共役でないと仮定する．$\mathfrak{q}'$ と $\sigma(\mathfrak{p}')$ $(\sigma \in G)$ は極大イデアルで互いに異なるから，$\sigma(\mathfrak{p}') \not\subset \mathfrak{q}'$ である．

ここで，次の補題を必要とする．

補題 1（素イデアルからの隔離の補題）． R を環，$\mathfrak{p}_1, \ldots, \mathfrak{p}_q$ を R の有限個

の素イデアル，$\mathfrak{b}$ を R のイデアルで $\mathfrak{b} \not\subset \mathfrak{p}_i$ $(i = 1, \dots, q)$ とする．このとき，$b \in \mathfrak{b}$ で $b \notin \mathfrak{p}_i (i = 1, \dots, q)$ となるものが存在する．

補題の証明 $\mathfrak{p}_j \not\subset \mathfrak{p}_i$ $(i \neq j)$ と仮定しても一般性は損なわれない．$x_{ij} \in \mathfrak{p}_j \setminus \mathfrak{p}_i$ $(i \neq j, 1 \leq i, j \leq q)$ とする．$\mathfrak{b} \not\subset \mathfrak{p}_i$ であるから，$a_i \in \mathfrak{b} \setminus \mathfrak{p}_i$ が存在する．$b_i = a_i \prod_{j \neq i} x_{ij}$ とおく．このとき，$b_i \in \mathfrak{b}$, $b_i \in \mathfrak{p}_j$ $(j \neq i)$, $b_i \notin \mathfrak{p}_i$（$\mathfrak{p}_i$ は素イデアルであるから）となる．従って $b = b_1 + \cdots + b_q$ とおくと，$b \in \mathfrak{b}$ で $b \equiv b_i \pmod{\mathfrak{p}_i}$ であるから，$b \in \mathfrak{b} \setminus \bigcup_{i=1}^{q} \mathfrak{p}_i$（よって，任意の $i = 1, \dots, q$ に対して $b \notin \mathfrak{p}_i$）となる．

命題の証明に戻る．補題から，元 $x \in \mathfrak{q}'$ があって，任意の $\sigma \in G$ に対して $x \notin \sigma(\mathfrak{p}')$ となる．x のノルム $\mathrm{N}(x) = \prod_{\tau \in G} \tau(x)$ を考える（2.6 節命題 1）．(1) より任意の $\tau \in G$ に対して $\tau(x) \in A'$ であるから，$\mathrm{N}(x) \in \mathfrak{q}'$ がわかる．実際，

$$\mathrm{N}(x) \in \mathfrak{q}' \cap A = \mathfrak{p}$$

である．他方，$x \notin \tau^{-1}(\mathfrak{p}')$ より任意の $\tau \in G$ に対して $\tau(x) \notin \mathfrak{p}'$ となる．$\mathfrak{p}'$ は素イデアルであることより，$\mathrm{N}(x) \notin \mathfrak{p}'$ となる．これは $\mathrm{N}(x) \in \mathfrak{p}$ に矛盾する． □

さて，$\mathfrak{p}'$ を A' の極大イデアルで $\mathfrak{p}' \cap A = \mathfrak{p}$ となるものとする．$\sigma \in G$ で $\sigma(\mathfrak{p}') = \mathfrak{p}'$ となるもの全体は G の部分群 D をなす．これは $\mathfrak{p}'$ の**分解群** (decomposition group) とよばれる．g を $\mathfrak{p}'$ と共役なものの個数とすれば

$$g = \mathrm{card}(G)/\mathrm{card}(D) \quad \text{すなわち}, \mathrm{card}(D) = n/g = ef \tag{2}$$

である．

$\sigma \in D$ に対して，$\sigma(A') = A'$, $\sigma(\mathfrak{p}') = \mathfrak{p}'$ という関係は σ が $A'/\mathfrak{p}'$ の自己同型 $\overline{\sigma}$ を与えることを示している（$x \equiv y \pmod{\mathfrak{p}'}$ より $\sigma(x) \equiv \sigma(y) \pmod{\mathfrak{p}'}$ が導かれる）．明らかに $\overline{\sigma}$ は $A/\mathfrak{p}$-自己同型である．写像 $\sigma \mapsto \overline{\sigma}$ は群の準同型で，その核は，任意の $x \in A'$ について $\sigma(x) - x \in \mathfrak{p}'$ が成り立つ $\sigma \in D$ からなる部分群 $I \subset D$ である．よって，I は D の正規部分群であり，$\mathfrak{p}'$ の**惰性群** (inertia group) とよばれる．

命題 2. 上記と同じ記号の下で，$A/\mathfrak{p}$ は有限体または標数 0 の体とする．このとき，$A'/\mathfrak{p}'$ は $A/\mathfrak{p}$ の f 次の Galois 拡大で，写像 $\sigma \mapsto \overline{\sigma}$ は D から $A'/\mathfrak{p}'$ の $A/\mathfrak{p}$ 上の Galois 群への全射準同型である．さらに $\mathrm{card}(I) = e$ である．

証明　K_D を D の不変体，$A_D = A' \cap K_D$ を A の K_D における整閉包，$\mathfrak{p}_D$ を素イデアル $\mathfrak{p}' \cap A_D$ とする．命題 1 と D の定義より，$\mathfrak{p}'$ は $\mathfrak{p}_D A'$ の唯 1 つの素因子である．$\mathfrak{p}_D A' = \mathfrak{p}'^{e'}$ とおき，f' を剰余次数 $[A'/\mathfrak{p}' : A_D/\mathfrak{p}_D]$ とする．5.2 節の定理 1，6.1 節の定理 2 と (2) より，

$$e'f' = [K' : K_D] = \mathrm{card}(D) = ef$$

を得る．$A/\mathfrak{p} \subset A_D/\mathfrak{p}_D \subset A'/\mathfrak{p}'$ であるから $f' \leq f$ である．$\mathfrak{p}A_D \subset \mathfrak{p}_D$ なので $e' \leq e$．従って，$e'f' = ef$ より $e = e'$ と $f = f'$ がわかる．これより

$$A/\mathfrak{p} \cong A_D/\mathfrak{p}_D \tag{3}$$

を得る．

さて，$\overline{x}$ を $A'/\mathfrak{p}'$ の $A/\mathfrak{p}$ 上の原始元とし，$x \in A'$ を $\overline{x}$ の代表元とする．$X^r + a_{r-1}X^{r-1} + \cdots + a_0 = P(X)$ を x の K_D 上の最小多項式とする．このとき $a_i \in A_D$ である（2.6 節命題 2 の系）ことはわかっている．$P(X)$ の根はすべて $\sigma(x)$ $(\sigma \in D)$ の形である．「簡約化された」多項式 $\overline{P}(X) = X^r + \overline{a}_{r-1}X^{r-1} + \cdots + \overline{a}_0$ は係数を $A/\mathfrak{p}$ にもち（(3) による），$\overline{P}(X)$ の根はすべて $\overline{\sigma}(\overline{x})$ $(\sigma \in D)$ の形である．従って $A'/\mathfrak{p}'$ は $\overline{x}$ の $A/\mathfrak{p}$ 上の共役元をすべて含み，$A'/\mathfrak{p}'$ は $A/\mathfrak{p}$ の Galois 拡大である（6.1 節定理 1(c)）．さらに $\overline{x}$ の $A/\mathfrak{p}$ 上の共役元はすべて $\overline{\sigma}(\overline{x})$ の形であり，$A'/\mathfrak{p}'$ の $A/\mathfrak{p}$-自己同型はすべて $\overline{\sigma}$ $(\sigma \in D)$ の形である．よって $A'/\mathfrak{p}'$ の $A/\mathfrak{p}$ 上の Galois 群は D/I と同一視できる．その位数は $[A'/\mathfrak{p}' : A/\mathfrak{p}] = f$ であるから，$\mathrm{card}(D)/\mathrm{card}(I) = f$．よって (2) より $\mathrm{card}(I) = e$ を得る．　□

系. $\mathfrak{p}$ が A' で分岐しないためには，$\mathfrak{p}$ 上にある任意の $\mathfrak{p}'$（すなわち，$\mathfrak{p}' \cap A = \mathfrak{p}$）に対して $\mathfrak{p}'$ の惰性群 I が自明（すなわち，$\{1\}$）であることが必要十分である．

注意. A' の極大イデアル $\mathfrak{p}'$ に対して，$D_{\mathfrak{p}'}, I_{\mathfrak{p}'}$ をそれぞれ $\mathfrak{p}'$ の分解群，惰

性群を表すものとする．共役イデアル $\sigma(\mathfrak{p}')$ $(\sigma \in G)$ に対して

$$D_{\sigma(\mathfrak{p}')} = \sigma D_{\mathfrak{p}'} \sigma^{-1}, \quad I_{\sigma(\mathfrak{p}')} = \sigma I_{\mathfrak{p}'} \sigma^{-1} \tag{4}$$

である．(4) を証明するためには，$\tau \in D_{\mathfrak{p}'}$ に対して

$$\sigma\tau\sigma^{-1} \cdot \sigma(\mathfrak{p}') = \sigma\tau(\mathfrak{p}') = \sigma(\mathfrak{p}')$$

が成り立ち，これより $\sigma D_{\mathfrak{p}'} \sigma^{-1} \subset D_{\sigma(\mathfrak{p}')}$ が出ることに注意しよう．

逆の包含関係は (1) の次に続くところで述べた注意と類似の議論により出る．同様にして，$\tau \in I_{\mathfrak{p}'}$ と $x \in A'$ に対して，

$$\sigma\tau\sigma^{-1}(x) - x = \sigma\tau(\sigma^{-1}(x)) - \sigma\sigma^{-1}(x) = \sigma(\tau(\sigma^{-1}(x)) - \sigma^{-1}(x)) \in \sigma(\mathfrak{p}')$$

が成り立つから，$\sigma I_{\mathfrak{p}'} \sigma^{-1} \subset I_{\sigma(\mathfrak{p}')}$ が出る．逆の包含関係は前と同じように考えればよい．

K' が K の Abel 拡大のとき，群 $D_{\sigma(\mathfrak{p}')}$ （または $I_{\sigma(\mathfrak{p}')}$）$(\sigma \in G)$ はすべて等しい．このことは環 A のイデアル $\mathfrak{p}$ にのみ依存する（命題 1）．

6.3 数体の場合．Frobenius 自己同型

前節の議論を数体とその整数環に応用してみよう．数体は標数 0 でその剰余体は有限体であるから，この応用は可能である．

前に用いた記号を用いることにする（すなわち，$K \subset K'$ はどちらも数体，K' は K の Galois 拡大で，その Galois 群を G，それぞれの整数環を A, A' とする）．$\mathfrak{p}$ を A の極大イデアルで A' において分岐しないものとし，$\mathfrak{p}'$ を $\mathfrak{p}A'$ の素因子とする．$\mathfrak{p}'$ の惰性群は G の単位元のみからなり（6.2 節命題 2 の系），その分解群 D は標準的に $A'/\mathfrak{p}'$ の $A/\mathfrak{p}$ 上の Galois 群と同型になる（6.2 節命題 2）．ところで $A'/\mathfrak{p}'$ の $A/\mathfrak{p}$ 上の Galois 群は標準的生成元 $\overline{\sigma} : \overline{x} \mapsto \overline{x}^q$ $(q = \mathrm{card}(A/\mathfrak{p}))$ をもつ巡回群である（6.1 節例 3）．従って D は巡回群であり，任意の $x \in A'$ に対して $\sigma(x) \equiv x^q \pmod{\mathfrak{p}'}$ をみたす標準的な生成元 σ が定義される．この生成元は $\mathfrak{p}'$ の **Frobenius 自己同型**とよばれる．これを $(\mathfrak{p}', K'/K)$ で表す．

6.2 節の最後の注意のところで述べたように，$\tau \in G$ に対して

$$(\tau(\mathfrak{p}'), K'/K) = \tau \cdot (\mathfrak{p}', K'/K) \cdot \tau^{-1} \tag{1}$$

が成り立つ．特に，K' が Abel 拡大ならば，$(\mathfrak{p}', K'/K)$ は A のイデアル $\mathfrak{p}$ にのみ依存する．この場合は $\left(\frac{K'/K}{\mathfrak{p}}\right)$ と表す．

命題 1. 上記の仮定と記号の下で，F を中間体 $(K \subset F \subset K')$ とし，f を $\mathfrak{p}' \cap F$ の K 上の剰余次数とする．このとき，

(a) $(\mathfrak{p}', K'/F) = (\mathfrak{p}', K'/K)^f$,

(b) F が K の Galois 拡大ならば，$(\mathfrak{p}', K'/K)$ の F への制限は $(\mathfrak{p}' \cap F, F/K)$ に等しい．

証明 (a) $\sigma = (\mathfrak{p}', K'/K)$ とおく．定義より，$\sigma(\mathfrak{p}') = \mathfrak{p}'$，また任意の $x \in A'$ に対して $\sigma(x) \equiv x^q \pmod{\mathfrak{p}'}$ （ここで $q = \mathrm{card}(A/\mathfrak{p})$）である．よって，任意の $x \in A'$ に対して

$$\sigma^f(\mathfrak{p}') = \mathfrak{p}', \quad \sigma^f(x) \equiv x^{q^f} \pmod{\mathfrak{p}'}$$

が成り立つ．f の定義より，q^f は剰余体 $(A' \cap F)/(\mathfrak{p}' \cap F)$ の濃度に等しい．さらに，$\mathfrak{p}'$ の F 上の分解群は明らかに，$\mathfrak{p}'$ の K 上の分解群 D の部分群である．その位数は 6.2 節 (2) より，

$$[A'/\mathfrak{p}' : (A' \cap F)/(\mathfrak{p}' \cap F)] = f^{-1}[A'/\mathfrak{p}' : A/\mathfrak{p}] = f^{-1} \cdot \mathrm{card}(D)$$

である．D は巡回群で，σ により生成されるから，位数が $f^{-1} \cdot \mathrm{card}(D)$ である D の部分群は σ^f によって生成されたもの唯 1 つである．これで (a) が示された．

(b) F を K の Galois 拡大とし，σ の F への制限を σ' と表す（6.1 節定理 2(b)）．$\sigma(\mathfrak{p}') = \mathfrak{p}'$ であるから，$\sigma'(\mathfrak{p}' \cap F) = \mathfrak{p}' \cap F$ であって，σ' は $\mathfrak{p}' \cap F$ の K 上の分解群に属す．さらに，任意の $x \in A' \cap F$ に対して $\sigma'(x) \equiv x^q \pmod{\mathfrak{p}' \cap F}$ が成り立つことは明らかで，$q = \mathrm{card}(A/\mathfrak{p})$ であった．以上で (b) が示された． □

6.4 円分体への応用

円分多項式の既約性についての第3の証明のところでちょうど展開していた理論を使うことにしよう（2.9節定理1と5.3節例を参照）．

定理 1. z を複素数の1の原始 n 乗根とする．このとき，

(a) n を割り切らない素数は $\mathbb{Q}[z]$ において分岐しない，

(b) $\mathbb{Q}[z]$ は $\mathbb{Q}$ の Abel 拡大で，次数は $\varphi(n)$，Galois 群は $(\mathbb{Z}/n\mathbb{Z})^*$ に同型である．

証明 (a) $F(X)$ を z の $\mathbb{Q}$ 上の最小多項式とし，d をその次数とする（このとき $d = [\mathbb{Q}[z] : \mathbb{Q}]$ である）．多項式 $F(X)$ は $X^n - 1$ を割り切るので，$X^n - 1 = F(X)G(X)$ とする．ここで $D(1, z, \ldots, z^{d-1}) = \pm \mathrm{N}(F'(X))$ がわかっている（2.7節(6)）．$nX^{n-1} = F'(X)G(X) + F(X)G'(X)$ であるから，z を代入して $nz^{n-1} = F'(z)G(z)$ が得られる．z は $\mathbb{Q}[z]$ の単数であるから，それはノルム ± 1 をもつ．ノルムをとると，$\mathrm{N}(F'(z))$ が n^d を割り切ることがわかる．結局，z は $\mathbb{Q}[z]$ の整数であるから，$\mathbb{Q}[z]$ の絶対判別式が $D(1, z, \ldots, z^{d-1})$ を割り切り，従って n^d も割り切る．5.3節の定理1より，n を割り切らない素数は $\mathbb{Q}[z]$ で分岐しないことがいえた．これで(a)が証明された．

(b) $\mathbb{Q}[z]$ が $\mathbb{Q}$ の Abel 拡大であり，$\mathbb{Q}[z]$ の $\mathbb{Q}$ 上の Galois 群 G から $(\mathbb{Z}/n\mathbb{Z})^*$ への単射準同型 j をもつことを思い出そう（6.1節例2）．もっと詳細にいえば，元 $\sigma \in G$ は1の n 乗根を $j(\sigma)$ 乗する．p を素数で n を割り切らないものとする．(a)より Frobenius 自己同型 $\left(\frac{\mathbb{Q}[z]/\mathbb{Q}}{p}\right)$ が定義されるから，それを σ_p と書こう．A を $\mathbb{Q}[z]$ の整数環，$\mathfrak{p}$ を pA の任意の素因子とすると，Frobenius 自己同型の定義より，任意の $x \in A$ に対して $\sigma_p(x) \equiv x^p \pmod{\mathfrak{p}}$ が成り立つ．特に，$j = j(\sigma_p)$ とおくとき，$z^j \equiv z^p \pmod{\mathfrak{p}}$ を得る．次の関係式を思い出そう．

$$\prod_{\substack{0 \leq r \leq n-1 \\ r \not\equiv p \pmod{n}}} (z^p - z^r) = P'(z^p) = nz^{p(n-1)},$$

ここで $P(X) = X^n - 1 = \prod_{0 \le r \le n-1}(X - z^r)$ である．n は p と互いに素で，$\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ であり，そして z は $\mathbb{Q}[z]$ の整数環の単元であるから，$P'(z^p) = nz^{p(n-1)}$ より，

$$\prod_{\substack{0 \le r \le n-1 \\ r \not\equiv p \pmod{n}}} (z^p - z^r) \notin \mathfrak{p}$$

を得る．$z^j \equiv z^p \pmod{\mathfrak{p}}$ であることは，j が p の n を法とする剰余類を代表していることを示している．ゆえに $j(G)$ は，n を割り切らないすべての素数 p の n を法とする剰余類を含んでいる．ところで，これは $j(G) = (\mathbb{Z}/n\mathbb{Z})^*$ を意味していて，(b) が証明された．□

6.5　平方剰余の相互法則の別証明

q を奇素数とする．K を円分体で，$\mathbb{C}$ の中で 1 の原始 q 乗根によって生成されているとする．K の $\mathbb{Q}$ 上の Galois 群 G は $\mathbb{F}_q^*$ と同型であり（6.4 節定理 1(b)），偶数位数 $q-1$ の巡回群である．指数 2 である部分群 H が唯 1 つ存在し，これは平方数からなる部分群 $(\mathbb{F}_q^*)^2 \subset \mathbb{F}_q^*$ に対応している．よって K は 2 次部分体 F を唯 1 つ含む（6.1 節定理 2(b)）．素数 $p \neq q$ は F において分岐しない．なぜならば，もしそうでないとすれば，p は K においても分岐してしまい，6.4 節の定理 1(a) に矛盾してしまうからである．2 次体の判別式の計算（5.3 節例 1）によって，$q \equiv 1 \pmod 4$ ならば $F = \mathbb{Q}[\sqrt{q}]$ であり，$q \equiv 3 \pmod 4$ ならば $F = \mathbb{Q}[\sqrt{-q}]$ であることを示している．$q^* = (-1)^{\frac{q-1}{2}}q$ とおけば，どちらの場合でも $F = \mathbb{Q}[\sqrt{q^*}]$ と書ける．

p を q と異なる素数とする．Frobenius 自己同型 $\left(\frac{K/\mathbb{Q}}{p}\right)$（6.4 節を参照）を σ_p と表す．σ_p の F への制限は $\left(\frac{F/\mathbb{Q}}{p}\right)$ である（6.3 節命題 1(b)）．もし $\sigma_p \in H$，すなわち，指数 $j(\sigma_p) =$「p の法 q についての剰余類」が $\mathbb{F}_q^*$ の中で平方であるならば，$\left(\frac{F/\mathbb{Q}}{p}\right)$ は恒等写像である．もしそうでない場合は，F の自明でない自己同型である．言い換えると，F の $\mathbb{Q}$ 上の Galois 群 G/H を（乗法群）$\{+1, -1\}$ と同一視すれば，Legendre の記号 $\left(\frac{p}{q}\right)$ の定義（5.5 節）より

$$\left(\frac{F/\mathbb{Q}}{p}\right)=\left(\frac{p}{q}\right) \tag{1}$$

を得る．

一方，素数 p の $F=\mathbb{Q}[\sqrt{q^*}]$ での分解に関する結果（5.4 節）は，$\left(\frac{F/\mathbb{Q}}{p}\right)$ についての情報をさらに与えてくれる．定義より，もし p が F で分解すれば，これは恒等写像であり，もし p が素を保つならばこれは自明でない自己同型である．5.4 節の命題 1 を用いると，p が奇素数ならば

$$\left(\frac{F/\mathbb{Q}}{p}\right)=\left(\frac{q^*}{p}\right) \tag{2}$$

を得る．

(1)，(2) を比較すると

$$\left(\frac{p}{q}\right)=\left(\frac{q^*}{p}\right)=\left(\frac{-1}{p}\right)^{\frac{q-1}{2}}\left(\frac{q}{p}\right)$$

となる．ところで，Euler の判定法（5.5 節命題 1）より

$$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$$

であるので，ゆえに

$$\left(\frac{p}{q}\right)=(-1)^{\frac{(p-1)(q-1)}{4}}\left(\frac{q}{p}\right)$$

を得る．これで平方剰余の相互法則（5.5 節定理 1）の第 2 の証明ができた．

$p=2$ の場合を扱うためには，もし $q^*\equiv 1 \pmod 8$ ならば 2 は F で分解し，もし $q^*\equiv 5 \pmod 8$ ならば 2 は素を保つこと（5.4 節命題 1）を思い出せばよい．ところで $(-1)^{\frac{q^2-1}{8}}=(-1)^{\frac{q^{*2}-1}{8}}$ であり，もし $q^*\equiv 1 \pmod 8$ なら，これは 1，もし $q^*\equiv 5 \pmod 8$ ならば，これは -1 である．よって

$$\left(\frac{F/\mathbb{Q}}{2}\right)=(-1)^{\frac{q^2-1}{8}} \tag{3}$$

を得る．(1) と (3) をまとめると，

$$\left(\frac{2}{q}\right)=(-1)^{\frac{q^2-1}{8}}$$

が成り立つ．これは，難解な「補充公式」（5.5 節命題 2(b)）であった．

練習問題

1*. (a) 体 $L=\mathbb{Q}[\sqrt{5},\sqrt{-1}]$ は $\mathbb{Q}$ の 4 次の Galois 拡大であることを示せ．その Galois 群を決定せよ．

(b) L の整数環 A は $\mathbb{Z}[\sqrt{-1},(1+\sqrt{5})/2]$ であることを示せ（ヒント：$\{1,(1+\sqrt{5})/2\}$ の Gauss 環上の判別式は平方因子をもたない（すなわち，平方因子をもつ Gauss の整数はない）ことに注意する．そして，5.3 節の命題 1 のアイディアを用いる）．L の絶対判別式を計算せよ．L において分岐する素数は 2 と 5 のみであり，分岐指数はともに 2 であることを示せ（ヒント：$n=efg$ を用いる．6.2 節命題 1 を参照）．

(c) p を 2 と 5 と異なる素数とするとき，Frobenius 自己同型 $\left(\frac{L/\mathbb{Q}}{p}\right)$ を計算せよ（ヒント：6.3 節を参照）．2 と 5 について分解群と惰性群を計算せよ．

(d) $\mathbb{Q}[\sqrt{-5}]\subset L$ であること，そして $\mathbb{Q}[\sqrt{-5}]$ のどの素イデアルも L で分岐しないことを示せ．

(e) 同様に，$\mathbb{Q}[\sqrt{10}]\subset\mathbb{Q}[\sqrt{2},\sqrt{5}]$ であることと，$\mathbb{Q}[\sqrt{10}]$ のどの素イデアルも $\mathbb{Q}[\sqrt{2},\sqrt{5}]$ では分岐しないことを示せ．

> ∞ $K=\mathbb{Q}[\sqrt{-5}],\mathbb{Q}[\sqrt{10}]$ は上のことより，ともに「不分岐」な Abel 拡大（すなわち，K のどの素イデアルも分岐しない）で，その Galois 群（位数 2 の巡回群）は K のイデアル類群と同型である．これは有名な「類体論」の非常に特殊な場合である．

2*. x を X^3-X+1 の実数根，y と $\overline{y}$ を $\mathbb{C}$ での他の 2 つの根とする．K を 3 次拡大 $\mathbb{Q}[x]$（5.3 節例を参照）とする．

(a) $y+\overline{y}=-x$, $y\overline{y}=-1/x$, $((y-x)(\overline{y}-x)(y-\overline{y}))^2=-23$ であることを示せ（ヒント：2.7 節公式 (6)，(7) を参照）．これより $K[\sqrt{-23}]=\mathbb{Q}[x,y,\overline{y}]$ とこの体 L は $\mathbb{Q}$ の 6 次の Galois 拡大であることを結論づけよ．その Galois 群 G を決定せよ（ヒント：L の $\mathbb{Q}$-自己同型は $x,y,\overline{y}$ への作用で定まることに注意する）．

(b) G の部分群は何か？ それらに対応する L の部分体を決定せよ（ヒント：6.1 節定理 2 を参照）．$\mathbb{Q}$ の Galois 拡大であるような L の部分体は何か？

(c) K の整数環は $\mathbb{Z}[x]$ であった（5.3 節最後の例）．$\mathbb{Z}[x]$ が単項イデアル環であることを示せ（ヒント：4.3 節命題 1 の系 1）．

(d) 23 が L において分岐する唯 1 つの素数であること，その分岐指数は 2 であることを示せ（ヒント：K の整数環における 23 の素因子分解は $\alpha\beta^2$ の形であることに注意する．6.2 節の命題 1 で定義された数で 23 の L における分解に関するものを e,f,g とすると，$g\geq 2$ で e は偶数（ヒント：第 V 章問題 8 を参照）であることを導け．$efg=6$ であることを用いて，$e=2,f=1,g=3$ を結論づけよ）．

(e) $\mathbb{Q}[\sqrt{-23}]\subset L$ であること，$\mathbb{Q}[\sqrt{-23}]$ のどの素イデアルも L では分岐しないこ

とを示せ．

∞ L は $\mathbb{Q}[\sqrt{-23}]$ の 3 次の巡回不分岐拡大であること，$\mathbb{Q}[\sqrt{-23}]$ のイデアル類群は位数 3 の巡回群であること（第 V 章問題 7(f) を参照）を調べよ．これは類体論のもう 1 つの特殊な場合である．

3*. 問題 2 を（$X^3 - X + 1$ の代わりに）多項式 $X^3 + X + 1$,（-23 の代わりに）-31 に置き換えよ．第 V 章問題 7(f) を $\mathbb{Q}[\sqrt{-31}]$ に置き換えよ．

4*. K を数体，L を K^* の $\mathbb{R}^{r_1+r_2}$ への対数的埋め込み（4.4 節定理 1）とする．K の単数群を U と表し，4.4 節の定理 1 で考えた超平面 W の格子 $L(U)$ の体積（写像 $W \to \mathbb{R}^{r_1+r_2-1}$ による Lebesgue 測度から導入された W での測度に関して）を K の**単数基準** (regulator) という．
(a) 4.6 節の中で明確な例として与えられていた実 2 次体の単数基準を計算せよ．
(b) z を $\mathbb{C}$ における 1 の原始 n 乗根，K を円分体 $\mathbb{Q}[z]$，σ を $\sigma(z) = z^{-1}$ で定義された K の自己同型，K' を σ の不変体とする．$[K : K']$ と，K と K' のそれぞれの単数群 U と U' の階数を計算せよ．これらの階数は同じ整数 r に等しいことを示せ．K と K' の単数基準をそれぞれ ρ, ρ' とするとき，ある整数 m があって，$\rho' = m\rho$ が成り立つことを示せ．K（あるいは，K'）に含まれる 1 のべき根の個数を計算せよ（ヒント：z として $e^{2i\pi/n}$ をとってよい）．U' の U における指数を決定せよ．
(c) (b) の記号の下で，$n = p^s$（p は素数で，$\neq 2$）と仮定する．$u \in U$ に対して $\sigma(u) = \pm z^{2j}u$ であること（ヒント：$\sigma(u)u^{-1}$ は任意の K の $\mathbb{C}$ への埋め込みについて，絶対値 1，よって 1 のべき根である），従って $\sigma(z^j u) = \pm z^j u$ であることを示せ．さらに $\sigma(z^j u) = z^j u$ であることを示せ（ヒント：$z^j u$ の K' 上の共役を考えることにより負の記号は取り除ける）．V を K に含まれる 1 の n 乗根の群とするとき，$U = V \cdot U'$ となることを導け．(b) の整数 m は 1 に等しいことを示せ．

5*. (a) K を 1 の 9 乗根 z によって $\mathbb{Q}$ 上生成された円分体とする．K は $\mathbb{Q}$ の 6 次の巡回拡大であることを示せ（ヒント：6.4 節を参照）．
G を Galois 群とする．
(b) G の指数 3 である部分群 H を用いて，$\mathbb{Q}$ の 3 次の Galois 拡大 K' を構成せよ（ヒント：6.1 節定理 2 を参照）．$K' = \mathbb{Q}[\cos\frac{2\pi}{9}]$ を示し，$2\cos\frac{2\pi}{9}$ の $\mathbb{Q}$ 上の最小多項式を決定せよ（ヒント：最小多項式は根として $z + z^8$, $z^2 + z^7$, $z^4 + z^5$ をもつ）．

補　足

この補足においては，証明なしで，本書で論じていたアイディアを補完したり一般化するような定義や事実についていくつか述べることにしよう．ここで導入される概念は本書の中で対応していた内容に比べて，そんなに難解とか困難であるというものではない．著者は本書を短編にまとめるために，本文の中でこれらの内容について詳しく論ずることを留保していたのである．それに，読者は多数の参考文献によって，より一般的な結果を見いだせることと思う（たとえば，[9] の第 V 章を参照せよ．本書の後ですぐに読まれるとよいであろう）．

本書の視野を越えたところにある数論における発展（アデール，類体，ゼータ関数，L-級数，単純環の数論，解析的数論，2 次形式，等々）をここに証明なしでまとめることは著者の意図するところではない．著者は参考文献の最初の部分（タイトルに番号を付けていないもの）で引用した仕事を読者自らが参照される方が，より好ましいことだと思っている．

推移公式 (transitivity formulas)

3 つの体 $K \subset L \subset M$ の各拡大が有限次であるものが与えられたとき,「トレース」写像

$$\mathrm{Tr}_{L/K} : L \to K,\quad \mathrm{Tr}_{M/L} : M \to L,\quad \mathrm{Tr}_{M/K} : M \to K$$

があり，同様に「ノルム」写像（2.6 節）もある．任意の $x \in M$ について，次の関係式が成り立つ．

$$\begin{cases} \mathrm{Tr}_{M/K}(x) = \mathrm{Tr}_{L/K}(\mathrm{Tr}_{M/L}(x)) \\ \mathrm{N}_{M/K}(x) = \mathrm{N}_{L/K}(\mathrm{N}_{M/L}(x)). \end{cases} \tag{1}$$

イデアルの相対ノルム (relative norm of an ideal)

2 つの数体 $K \subset K'$ と K' の（整または分数）イデアル $\mathfrak{a}'$ が与えられたとき，$\mathrm{N}_{K'/K}(x)$ $(x \in \mathfrak{a}')$ の形の K の元全体によって生成された K のイデアルを $\mathfrak{a}'$ の**相対ノルム** (relative norm) という．それを $\mathrm{N}_{K'/K}(\mathfrak{a}')$（または $\mathrm{N}(\mathfrak{a}')$）で表す．もし $\mathfrak{a}'$ が単項イデアル (a') であれば，

$$\mathrm{N}_{K'/K}(\mathfrak{a}') = (\mathrm{N}_{K'/K}(a')) \tag{2}$$

である．もし $K = \mathbb{Q}$ ならばこのノルムの定義は 3.5 節で与えたものと一致する．すなわち，$\mathfrak{a}'$ が K' の整イデアルで，A' が K' の整数環ならば，

$$\mathrm{N}_{K'/\mathbb{Q}}(\mathfrak{a}') = \mathrm{card}(A'/\mathfrak{a}')\mathbb{Z} \tag{3}$$

である．

一般の場合に戻ろう．$\mathfrak{a}$ を K のイデアルで，$n = [K' : K]$ とすれば，

$$\mathrm{N}_{K'/K}(A'\mathfrak{a}) = \mathfrak{a}^n. \tag{4}$$

K' のイデアル $\mathfrak{a}', \mathfrak{b}'$ に対しては，次の乗法公式がある．

$$\mathrm{N}_{K'/K}(\mathfrak{a}'\mathfrak{b}') = \mathrm{N}_{K'/K}(\mathfrak{a}')\mathrm{N}_{K'/K}(\mathfrak{b}'). \tag{5}$$

最後に，$\mathfrak{p}'$ が K' の素イデアルで，$\mathfrak{p} = \mathfrak{p}' \cap K$ とし，f を $\mathfrak{p}'$ の K 上の剰余次数とすれば，

$$\mathrm{N}_{K'/K}(\mathfrak{p}') = \mathfrak{p}^f. \tag{6}$$

3 つの数体 $K \subset K' \subset K''$ に対して，次の推移公式が K'' の任意のイデアル $\mathfrak{a}''$ に対して成り立つ．

$$\mathrm{N}_{K''/K}(\mathfrak{a}'') = \mathrm{N}_{K'/K}(\mathrm{N}_{K''/K'}(\mathfrak{a}'')). \tag{7}$$

同じ流れで，イデアルの相対ノルムのことばを用いて，判別式の推移公式が得られる（ここで，$\mathfrak{D}_{K'/K}$ は K' の K 上の判別式を表す，5.3 節定義 1 を参照）．

$$\mathfrak{D}_{K''/K} = \mathrm{N}_{K'/K}(\mathfrak{D}_{K''/K'}) \cdot \mathfrak{D}_{K'/K}^{[K'':K']}. \tag{8}$$

上記のことは Dedekind 環 A と A の分数体の有限拡大の中での A の整閉包 A' の場合に一般化できる.

共役差積 (different)

次のことがらは Dedekind 環 A と A の分数体の有限拡大における A の整閉包についても成り立つが, 簡単のために, 数体の場合に議論を限ることにする.

K, K' を数体で $K \subset K'$ とする. A と A' をそれぞれ K と K' における整数環とする. A' の極大イデアル $\mathfrak{p}'$ は A 上の分岐指数が 1 より大きいとき, A 上 (または K 上) **分岐する**という. このとき A の極大イデアル $\mathfrak{p} = \mathfrak{p}' \cap A$ は A' において**分岐する**という (5.3 節). 5.3 節の定理 1 より, A' の極大イデアルで A 上分岐するものは有限個であることが容易にわかる. K' の K 上の「共役差積」(different) とよばれる A' のイデアル $\mathfrak{d}_{K'/K}$ について見ていくことにしよう. $\mathfrak{d}_{K'/K}$ には, A 上分岐する極大イデアル全体は $\mathfrak{d}_{K'/K}$ を含む極大イデアル全体と等しい, という性質がある (5.3 節の定理 1 との類似に注意せよ).

まず, 元 $x \in K'$ で次の関係

$$\mathrm{Tr}_{K'/K}(xA') \subset A \tag{9}$$

をみたすもの全体の集合は A' の分数イデアル $\mathfrak{C}$ である. これは K' の K 上の**共役余差積** (codifferent) とよばれる. **共役差積** (different) $\mathfrak{d}_{K'/K}$ を逆イデアル $\mathfrak{C}^{-1}$ と定義する. 共役差積は A' の (0) でない整イデアルである. x を A' の元, $F(X)$ を x の K 上の最小多項式, $F'(X)$ を F の導関数を表すものとするとき, 共役差積は, x を A' の中で動かしたときの $F'(x)$ の形の元全体によって生成される. 特に, A' が $A[y]$ の形 (必ずしもこの場合とは限らないが) のとき, $G(X)$ を y の K 上の最小多項式とすれば, 共役差積 $\mathfrak{d}_{K'/K}$ は $G'(y)$ によって生成される A' の単項イデアルである.

A 上分岐する A' の (0) でない素イデアル全体は $\mathfrak{d}_{K'/K}$ を含む素イデアル全体となる. より正確にいうために,

$$\mathfrak{d}_{K'/K} = \prod_i \mathfrak{p}_i'^{m_i} \quad (m_i > 0) \tag{10}$$

は共役差積を相異なる素イデアルのべきの積に分解したものとし，e_i を $\mathfrak{p}'_i$ の A 上の分岐指数とする．このとき，A' の (0) でない素イデアルで，A 上分岐するものは $\mathfrak{p}'_i$ で $m_i \geq e_i - 1$ であるものである．さらに，$m_i = e_i - 1$ となることは，e_i が剰余体 $A'/\mathfrak{p}'_i$ の標数と互いに素であるための必要十分条件である．

共役差積 $\mathfrak{d}_{K'/K}$（A' のイデアル）と判別式 $\mathfrak{D}_{K'/K}$（A のイデアル）は次の関係

$$\mathfrak{D}_{K'/K} = \mathrm{N}_{K'/K}(\mathfrak{d}_{K'/K}) \tag{11}$$

によりつながっている（2.7 節公式 (6) を参照）．よって共役差積は A と A' の素イデアルの分岐性について判別式よりも精密な情報を与えてくれる．

最後に，3 つの数体 $K \subset K' \subset K''$ に対して，共役差積について次の推移関係

$$\mathfrak{d}_{K''/K} = \mathfrak{d}_{K''/K'} \cdot \mathfrak{d}_{K'/K} \tag{12}$$

があることをいっておこう．

演習問題

I

複素数体 $\mathbb{C}$ において，$z = e^{2i\pi/5}$ とおき，K を円分体 $\mathbb{Q}(z)$ とする．

1. K の次数，整数環，絶対判別式を求めよ（ヒント：絶対判別式を計算するためには $\mathrm{Tr}(z^j)$ を計算すると便利である）．K の整数環 A において分岐する素数は何か？

2. $\mathbb{R}$ を実数体とし，$K' = K \cap \mathbb{R}$ とおく．K' は 2 次体であることを示し，それがどのようなものか決定せよ．K' の整数環 A' と A' の単数群 A'^* を記述せよ．

3. K' は K に含まれる唯 1 つの 2 次体であることを示せ（ヒント：K'' が K の部分体ならば，K'' で分岐するすべての素数は K において分岐することに注意する）．

4. K は 1 の 10 乗根を除いた 1 のべき根は含まないことを示せ（ヒント：位数が素数または 2 のべきであるような 1 のべき根を考え，問題 3 を用いれば十分である）．

G を 1 の 10 乗根のなす群とする．

5. (a) K の対数的埋め込みを用いて，K の整数環 A において a が絶対値 1 の単数ならば a は 1 のべき根であることを示せ．
(b) $a = re^{i\theta}$ を A の単数 $(r > 0)$ とする．$r^2 \in A'^*$，$e^{2i\theta} \in G$ であることを示せ．また，$r \in A'^*$ であることと $e^{i\theta} \in G$ であることが同値であることを示せ．
(c) $(1-z)A = (1-z^2)A = (1-z^3)A = (1-z^4)A$ は A の素イデアル $\mathfrak{p}$ で，$5A = \mathfrak{p}^4$ であった．$(1-z^3)K'$ のどの元も A の単数でないこと，A は偏角が $\pi/10$ である単数を含まないこと，A の単数群 A^* は G と A' の正の単数のなす群 U との直積であることを結論づけよ．

6. 以前に用いた記号の下で，数体の任意のイデアル類はノルム $\leq (4/\pi)^{r_2} n!\, n^{-n} |d|^{\frac{1}{2}}$ である整イデアルを含むことを思い出そう．環 A は単項イデアル環であることを示せ．

II

$\mathbb{Q}$ は有理数体，x を $x^3 = 2$ であるような実数，K を体 $\mathbb{Q}(x)$ とする．

1. 多項式 $X^3 - 2$ は $\mathbb{Q}$ 上で既約であること，K は $\mathbb{Q}$ の 3 次拡大であることを示せ．複素数体 $\mathbb{C}$ の中で K と共役な体は何か？

2. $z = a + bx + cx^2$ $(a, b, c \in \mathbb{Q})$ を K の元とする．z の $\mathbb{Q}$ 上のトレース，ノルム，固有多項式を計算せよ．

3. $\mathbb{Z}$ を有理整数環，B を K の部分環 $\mathbb{Z}[x]$ とする．この問題で，K の整数環 A が B に等しいことを示すことにしよう．
(a) $B \subset A$ であることを示し，B の $\mathbb{Z}$-加群としての基底を見つけよ．
(b) $z = a + bx + cx^2$ $(a, b, c \in \mathbb{Q})$ を K の整数とする．z, xz, x^2z のトレースを計算することにより，$6A \subset B$ であることを示せ．
　残りの証明については，問題 2 を用いることによって (b) で定義された整数 $6a, 6b, 6c$ が 6 の倍数であることを示してもよい（ヒント：議論は長くなるが，初等的である）．また，初等的ではなくなるが，次のように進むこともできよう．
(c) イデアル xA と xB が素イデアルであることを示せ（ヒント：xA についてはイデアル $2A$ を A の中で分解することを考える）．$xB = B \cap xA$ であること，体 A/xA と B/xB が一致することを示せ．$A = B + xA$，よって $A = B + 2A$ となることを結論づけよ．
(d) $3 = (x-1)(x+1)^3$ となること，$x - 1$ が B において可逆であることを示せ．(c) において x の代わりに $x + 1$，2 の代わりに 3 で置き換えて同様に考え，$A = B + (x+1)A$ を示し，結局，$A = B + 3A$ となることを示せ．
(e) (c) と (d) から，$A = B + 6A$ を導き，最後に $A = B$ を導け．

4. K の共役差積と判別式を計算せよ．

5. (a) A の単数群（乗法的）の構造は何か？ すべての正の単数（あるいは，負の単数）はノルムが 1（あるいは，-1）であることを示せ．$x^2 + x + 1$ が A の単数であることを示せ．
(b) もし u が A の単数 > 1 で，D が K の判別式ならば，$|D| < 4u^3 + 24$ であった（第 IV 章問題 3）．$x^2 + x + 1$ が K の正の単数のなす群の生成元であることを

結論づけよ（ヒント：x と x^2 の近似値は 1.26 と 1.58 である）．
(c) 方程式 $a^3+2b^3+4c^3-6abc=1$ の整数解 a,b,c を 3 つまたは 4 つ計算せよ．どうしたらすべての有理整数解を見いだせるか，またすべての正の整数解についてはどうかも説明せよ．

III

1. 多項式 X^3-3X+1 は $\mathbb{Q}$ の中で根をもたず，$\mathbb{Q}$ 上既約であることを示せ．$\mathbb{C}$ におけるその 3 つの根は実数であることを示せ．

x を問題 1 における根のうちの 1 つとする．K を 3 次体 $\mathbb{Q}[x]$，A を K の整数環とする．

2. 判別式 $D(1,x,x^2)$ を計算せよ．$a+bx+cx^2$ $(a,b,c\in\mathbb{Q})$ を K の整数とするとき，$a,b,c\in S^{-1}\mathbb{Z}$，ここで $S=\{3^n\}_{n\geq 0}$ である，ことを導け（ヒント：$S^{-1}\mathbb{Z}\subset S^{-1}A$ を考える）．

3. $A'=\mathbb{Z}[x]$ とおく．x と $x+2$ は A' と A の単数であること，$(x+1)^3=3x(x+2)$ であることを示せ．$(x+1)A$ は A の素イデアルであること，$(x+1)A\cap A'=(x+1)A'$ であること，$A/(x+1)A=A'/(x+1)A'$ であることを結論づけよ．$A=A'+(x+1)A$，そして $A=A'+3A$ であることを示せ．これと問題 2 より $A=A'=\mathbb{Z}[x]$ であることを結論づけよ．

4. $2A$ は A の素イデアルであることを示せ（ヒント：X^3-3X+1 は 2 を法として既約であることに注意する）．これより A は単項イデアル環であることを導け（ヒント：A の任意のイデアル類はノルム $\leq (4/\pi)^{r_2}(n!/n^n)|D|^{1/2}$（通常の記号の下で）である整イデアルを含むことを思い出そう）．

5. x^2-2 は多項式 X^3-3X+1 の根であることを示せ．$\mathbb{Q}$ 上 K と共役な体は何か？ K から $\mathbb{C}$ の中への $\mathbb{Q}$-同型は何か？

6. $\cos 3u=4\cos^3 u-3\cos u$ が成り立つことを思い出そう．$x=2\cos u$ とおいて，角 u のとれる値を計算せよ．L をある円分体とすると，K は $L\cap\mathbb{R}$ の形となることを結論づけよ．どんな円分体であるか決定せよ．

注意．問題 5, 6 は問題 2, 3, 4 と独立である．

参考文献

E. Artin, *Theory of algebraic numbers* (G. Striker, Schildweg 12, Göttingen, Germany–1957)（付値理論が展開されている．大変エレガント．例が豊富）．

H. Hasse, *Zahlentheorie* (Akademie Verlag, Berlin, 1949)（大部で大変完備な作品）．

H. Hasse, *Vorlesungen über Zahlen theorie* (Springer, 1964)（数論のいろいろな面を解説している）．

G. H. Hardy, E. M. Wright, *An introduction to the theory of numbers* (Clarendon Press, Oxford, 1965)（深淵で華麗．内容の選択において顕著に審美的なセンスを示している）．（[訳注] 邦語版は G. H. ハーディ，E. M. ライト，数論入門 I · II（示野信一，矢神毅訳），シュプリンガー・フェアラーク東京，2001.）

E. Hecke, *Vorlesungen über die Theorie der algebraischen Zahlen* (Chelsea, New York, 1948)（古典的．エレガントで完備している）．

S. Lang, *Algebraic numbers* (Addison–Wesley, 1964)（小さいが非常に中身の濃い本）．

S. Lang, *Diophantine geometry* (Interscience Tract no. 11, J. Wiley, New York, 1962)（Diophantus 方程式を指向．代数幾何学との関連をうまく示している）．

O'Meara, *Introduction to quadratic forms* (Springer, 1963)（代数的数論についての効力のある解説，その最も美しい応用と動機を伴っている）．

J. P. Serre, *Corps locaux* (Hermann, Paris, 1962), *Local fields* (Graduate Texts in Math. 67, Springer-Verlag, 1979)（p-進体に重点をおいている．数論における最近の代数的手法を明確にかつ明瞭に展開している．内容が大変豊富．たくさんの例）．

E. Artin, J. Tate, *Class-field theory* (W. A. Benjamin, 1968)（有名な類体論，すなわち，数体の Abel 拡大の理論の最も新しい展開）．

A. Weil, *Basic number theory* (Springer, 1967)（アデールの豊かな手法を用いるとともに，数体と関数体を同時に扱っている）．

Z. I. Borevich, I. R. Shafarevich, *Number theory* (Academic Press, 1966)（たいへん完備している．複素解析的方法と p-進解析的方法についてのすばらしい章がある．たくさんの数表）．

[1] N. Bourbaki, *Algèbre* (Paris, Hermann)（特に，体についての第 V 章，整除についての第 VI 章，単項イデアル環上の加群についての第 VII 章）．

[2] N. Bourbaki, *Algèbre commutative*（同上）（特に，環上の整元についての第 V 章，Dede-kind 環と一意分解環についての第 VII 章．第 II 章は分数環について論じられているが，完備で包括的である．付値論についてのよい解説が第 VI 章にある）．

[3] C. Carathéodory, *Theory of functions*, Vol. I (Chelsea, New York, 1954).

[4] S. Lang, *Algebraic structures* (Addison–Wesley, 1967).

[5] S. Lang, "On quasi-algebraic closure" (Ann. of Math., **55**(1962), 373–390).

[6] P. Samuel, "A propos du théorème des unités" (Bull. Sci. Math., **90**(1966), 89–96).

[7] P. Samuel, "Anneaux factoriels" (Publ. Soc. Math. São Paulo, 1964)（また，次の論文も参照のこと．"Unique factorization", American Math. Monthly, **75**(1968), 945–952）．

[8] G. Terjanian, "Sur une conjecture de M. Artin" (C. R. Acad. Sci. Paris, (1966)).

[9] O. Zariski, P. Samuel, *Commutative algebra*, Vol. I (Van Nostrand, Princeton, 1958)（第 II 章は体論，第 IV 章は Noether 環，そして第 V 章は環上の整元と Dedekind 環について論じられている）．

日本語の参考文献を追加しておこう（訳者）．

藤崎源二郎，森田康夫，山本芳彦，数論への出発（数学セミナー増刊），日本評論社，1980.

岩澤健吉，代数函数論，岩波書店，1973（改訂版）．

岩澤健吉，局所類体論，岩波書店，1980.

J. P. セール，数論講義（彌永健一訳），岩波書店，1979.

高木貞治，初等整数論講義，共立出版，1972（第二版）．

高木貞治，代数的整数論，岩波書店，1982（第二版）．

武隈良一，2 次体の整数論，槇書店，1966.

石田信，代数的整数論，森北出版，1974.

藤崎源二郎，代数的整数論入門（上），(下），裳華房，1975.

小野孝，数論序説，裳華房，1988.

河田敬義，数論，岩波書店，1992.

斎藤秀司，整数論，(共立講座 21 世紀の数学）共立出版，1999.

森田康夫，整数論，裳華房，1998.

山本芳彦，数論入門，(岩波講座現代数学への入門）岩波書店，1996.

加藤和也，黒川信重，斎藤毅，栗原将人，数論，(岩波講座現代数学の基礎）岩波書店，1999.

A. ヴェイユ，数論歴史からのアプローチ（足立恒雄，三宅克哉訳)，日本評論社，1987.

訳者はしがき

本書は P. Samuel の *Théorie Algébrique des Nombres* の第 2 版（1971 年）を翻訳したものである．原著者が前書きに書いているように，整数論の専門家ではなく，代数幾何学の研究者が書いたテキストである．それであるがゆえにかえって，代数学の，それも可換代数（代数幾何学の局所理論とも考えられる）の初歩を終えた人にとっては，それらの知識を整数論の世界で具体化してみるという意味でも，本書は適しているのではないだろうか．豊富な演習問題に取り組むことにより，代数的整数論の世界をかいま見ることができ，また整数論により多くの興味を起こされるであろう．

整数論のテキストとしては，日本語で書かれた比較的新しい良書がたくさんある（参考文献を参照）．そうした中にあって，本書原著の初版は 1967 年に発刊されているものだが，内容的には古さを感じさせるものはなく，代数学の方面から整数論を勉強するのに適していると思う．少なくとも初学者には類書と比較して近づき易いのではないだろうか．

原著では巻末にまとめてあった各章の練習問題は，この訳書では読者の便宜を考えて各章の終わりのところに分散されている．難しいと思われる問題には原著者がつけたヒントもそのまま訳しておいてあるので，できるだけ問題にチャレンジして欲しいと思う．

翻訳にあっては，訳語はできるだけ広く流布されているものを採用したつもりである．また，Allan Silberger の英語訳（1971 年）を大いに参考にして，できるだけわかりやすくなるように心がけた．そのために，フランス語版原著になく英訳者によって補足されたと考えられる箇所でも，適切と思わ

れるところは訳者の判断で断りなしに採用した部分があることを記しておく．

最後に，本書を翻訳するにあたって，シュプリンガー・フェアラーク東京の編集部に多大の御協力をいただいた．ここに感謝の意を表したい．

訳者記す —— 2005 年高知にて．

索　引

■記号索引

■欧字先頭和文索引

■和文索引

●あ行

●か行

著　者
P. サミュエル (Pierre Samuel)
1921 年生まれ．フランスの数学者集団ブルバキの第 2 世代のメンバーの一人として，1947 年から 1971 年まで活動．前パリ大学教授．著書として，本書の他に，ザリスキーとの共著 Commutative Algebra I, II (Springer-Verlag, GTM 28, 29) 等がある．

訳　者
織田　進（おだ　すすむ）
高知大学教育学部教授．博士（理学）．

シュプリンガー数学クラシックス　第 18 巻
数の代数的理論　　**定価（本体 2,700 円＋税）**

発　行　2005 年 12 月 22 日
著　者　P. サミュエル
訳　者　織田 進
発行者　深田 良治
発行所　シュプリンガー・フェアラーク東京株式会社
〒113-0033　東京都文京区本郷 3 丁目 3 番 13 号
TEL (03) 3812-0757 (営業直通)
印刷所　平河工業社

ISBN 4-431-71188-0　C3041　http://www.springer-tokyo.co.jp